



Implementation Guide

Public Health Information Network Messaging System (PHINMS)

Version: 2.8.01

**Prepared by:
U.S. Department of Health & Human Services**

Date: December 17, 2008



EXECUTIVE SUMMARY

Public health involves many organizations throughout the PHIN (Public Health Information Network), working together to protect and advance the public's health. These organizations need to use the internet to securely exchange sensitive data between varieties of different public health information systems. The exchange of data, also known as "messaging" is enabled through messages created using special file formats and a standard vocabulary. The exchange uses a common approach to security and encryption, methods for dealing with a variety of firewalls, and internet protection schemes. The system provides a standard way of addressing messages being routed securely while providing a consistent confirmation of message exchange.

The Public Health Information Network Messaging System (PHINMS) sends and receives sensitive data over the internet to the public health information systems using Electronic Business Extensible Markup Language (ebXML) technology securely.

The PHINMS Implementation Guide provides instructions for installation and basic configuration of the PHINMS 2.8.01 software; advance configuration procedures are located in the PHINMS Technical Guide.



REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
0.1	Lawrence Loftley	12-16-2008	Implemented 2.8.01 Implementation Guide.
0.2	Tavan Jones	12-16-2008	Review
0.3	Rajeev Seenappa	12-16-2008	Review
1.0	Tom Brinks	12-17-2008	Final review and approval

TABLE OF CONTENTS

1.0	Introduction.....	10
	References.....	10
	Communiqués	11
2.0	Installation Requirements	12
	2.1 PHINMS 2.8.01 Tests	12
	2.2 System Requirements	12
	2.3 Apply for a digital certificate:.....	13
	2.4 Request PartyID	13
3.0	Download & Install the PHINMS Software	15
4.0	Upgrade PHINMS Software	27
5.0	Configure SQL Databases.....	36
6.0	Sender Information.....	37
	6.1 Ping Loopback	38
	6.2 Ping CDC Ping Server	40
	6.3 Configure CDC Staging Receiver.....	42
	6.4 Email CPA File.....	45
	6.5 Ping CDC Staging Receiver	45
	6.6 Send Test Payload Message.....	47
	6.7 Create Route Map	50
	6.8 Key Store Management Export certificate wizard.....	51
	Key Store Management Import certificate wizard.....	56
7.0	Receiver Information.....	59
	7.1 Configure WorkerQ	59
	7.2 Create Service and Action Pair.....	62
	7.3 Configure Service Map.....	65
8.0	Uninstall PHINMS 2.8.01	67
9.0	Additional Features	69
	9.1 Export CPA.....	69
	9.2 Import CPA.....	69
	9.3 View Receiver Logs.....	69
	9.4 View Sender Logs.....	70
	9.5 Import Trusted Certificate	70
	9.6 Import JDBC JAR Files	70
	9.7 Change Login Password	71
	9.8 Sender and Receiver Alarms.....	71
	9.9 Alarm Resolution.....	72
	9.10 Folder-Based Polling	73
	9.11 Transport Queue Auto Delete	74
	9.12 Worker Queue Auto Delete	75

LIST OF FIGURES

Figure 3.1. Log On As	15
Figure 3.2. Phinms2.8.01 FTP downloads	15
Figure 3.3. Phinms2.8.01 open FTP site in Windows explorer	16
Figure 3.4. Phinms2.8.01 FTP downloads windows explorer view	16
Figure 3.5. Phinms2.8.01 FTP Windows Build	17
Figure 3.6. File Download - Security Warning.....	17
Figure 3.7. Opening PHINMS 2.8.01	17
Figure 3.8. Install Shield Wizard Preparation Screens	18
Figure 3.9. End User Agreement Screen	18
Figure 3.10. New Installation or Upgrade Screen.....	19
Figure 3.11. Directory Name Screen	19
Figure 3.12. The target directory will be created	20
Figure 3.13. PartyID and Domain Name Screen	20
Figure 3.14. Port Numbers Screen.....	21
Figure 3.15. Register this PHINMS instance with PHIN/CDC	21
Figure 3.16. Installation Package screen.....	22
Figure 3.17. Installation	22
Figure 3.18. Setup Shortcuts.....	23
Figure 3.19. PHINMS Installation Options	23
Figure 3.20. PHINMS Processing.....	24
Figure 3.21. PHINMS Installation Finished	24
Figure 3.22. PHINMS Welcome screen	25
Figure 3.23. PHINMS Console Login Screen	25
Figure 3.24. PHINMS Console.....	26
Figure 4.1. Install Shield Wizard Preparation Screens	27
Figure 4.2. End User Agreement Screen	28
Figure 4.3. New Installation or Upgrade Screen.....	28
Figure 4.5. The PHINMS 2.7.00 SP1 directory path	29
Figure 4.6. The PHINMS 2.7.00 SP1 directory path	30
Figure 4.7. Upgrade Location	30
Figure 4.8. Port Numbers Screen.....	31
Figure 4.9. Installation Package screen.....	31
Figure 4.10. Installation	32
Figure 4.11. Setup Shortcuts.....	32
Figure 4.12. PHINMS Installation Options	33
Figure 4.13. PHINMS Processing.....	33
Figure 4.15. PHINMS Installation Finished	34
Figure 4.16. PHINMS Welcome screen	34
Figure 4.17. PHINMS Console Login Screen	35
Figure 4.18. PHINMS Console.....	35
Figure 6.1. CDC PHINMS Topology	38
Figure 6.2. PHINMS 2.8.01 Console.....	39
Figure 6.3. PHINMS Ping.....	39

Figure 6.4. Ping Message.....	40
Figure 6.5. PHINMS 2.8.01 Console.....	41
Figure 6.6. PHINMS Ping.....	41
Figure 6.7. CDCPingServer Message	42
Figure 6.8. PHINMS 2.8.01 Console.....	42
Figure 6.9. Sender Configuration.....	43
Figure 6.10. Route Map Item	43
Figure 6.11. CDC Route Map Configuration.....	44
Figure 6.12. CDC Route Map.....	44
Figure 6.13. CDC Route Configuration Successful.....	45
Figure 6.14. PHINMS 2.8.01 Console.....	46
Figure 6.15. PHINMS Ping Message.....	46
Figure 6.16. Ping Message.....	47
Figure 6.17. PHINMS 2.8.01 Console.....	48
Figure 6.18. PHINMS Ping.....	48
Figure 6.19. Security Options	49
Figure 6.20. New Message Notification	49
Figure 6.21. PHINMS 2.8.01 Console.....	50
Figure 6.22. Route Map	50
Figure 6.23. Route Map Item	51
Figure 6.24. Route Map Item	52
Figure 6.25. Windows MMC Certificates.....	52
Figure 6.26. Certificate Export Wizard.....	53
Figure 6.27. Export Private Key	53
Figure 6.28. Export File Format	54
Figure 6.29. Password.....	54
Figure 6.30. File to Export.....	55
Figure 6.31. Save As.....	55
Figure 6.32. Export was Successful	55
Figure 6.33. Route Map Item	56
Figure 6.34. browse for .pfx file	56
Figure 6.36. Sender Configuration.....	57
Figure 6.37. Set Configuration.....	58
Figure 7.1. PHINMS 2.8.01 Console.....	59
Figure 7.2. Receiver Configuration - Database	60
Figure 7.3. Database Item	60
Figure 7.4. Queue Maps.....	61
Figure 7.5. Queue Map Item	62
Figure 7.6. WorkerQ Database Configuration Successful.....	62
Figure 7.7. PHINMS 2.8.01 Console.....	63
Figure 7.6. Service Map.....	63
Figure 7.7. Service Map Item	64
Figure 7.8. Service and Action Added.....	64
Figure 7.9. Service and Action Successful Configuration.....	65
Figure 7.10. PHINMS 2.8.01 Console.....	65



Figure 7.12. Service Map Receiver Configuration	65
Figure 7.13. Service Map Item	66
Figure 8.1. PHINMS Uninstaller screen	67
Figure 8.2. Application Uninstaller	67
Figure 8.3. Successful Uninstall	67
Figure 8.4. PHINMS install directory	68
Figure 9.2. Alarm Resolution.....	73
Figure 9.3. Alarm Successfully Processed.....	73



LIST OF TABLES

Table 1. JDBC Drivers.....	12
Table 2. WorkerQ Database Tag Values	61

ACRONYM LIST

CDC	Centers for Disease Control and Prevention
CPA	Collaboration Protocol Agreement
CPS	Certification Practice Statement
ebXML	Electronic Business Extensible Markup Language
FAQs	Frequently Asked Questions
FTP	File Transfer Protocol
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
PC	Personal Computer
PartyID	Party Identifier
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System
PHINMSG	Public Health Information Network Messaging
RDBMS	Relational Database Management System
SDN	Secure Data Network
SQL	Structured Query Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
TransportQ	Transport Queue
URL	Uniform Resource Locator
WorkerQ	Worker Queue

1.0 INTRODUCTION

The Public Health Information Network Messaging System (PHINMS) Implementation Guide will assist with the installation, configuration, and upgrade of the PHINMS product which is update periodically. Refer to the PHINMS website at www.cdc.gov/phn/phinms for the most current release of PHINMS software.

The PHINMS Implementation Guide provides instructions to correctly install and configure PHINMS to send and receive messages from the Centers for Disease Control and Prevention (CDC) and CDC partners. PHINMS Web Site Topics

- **Overview:** Contains a summary on the purpose of PHINMS. Announces new PHINMS features and processes.
- **Installation:** This section of the web site provides documentation pertinent to the installation and configuration the PHINMS software. Various other types of PHINMS documents are also available e.g. Acronym and Glossary List, Web Service Adapters, and many more.
- **Quick Steps:** PHINMS Quick Steps provide an overview of the information needed most often. The Quick Steps are documented for Release 2.8.01. Suggestions to add additional questions can be sent to the PHINMS Web Site point-of-contact using the Support tab.
- **FAQs:** The list of Frequently Asked Questions (FAQs) is stored in this section. The list contains answers to many questions users have previously submitted. The PHINMS Team welcomes questions, suggestions, and/or comments.
- **Support:** The Support section provides contact information for signing up to use the PHINMS Forum, contacting the Help Desk, accessing Online Help, and contacting the Web Site administrator.

References

NAME	LOCATION
Quick How Tos	Located at www.cdc.gov/phn/phinms .
PHINMS Release Notes 2.8.01	Description of supported environments, software requirements, explanation of upgrade path, and a list of new features and bug fixes made since PHINMS release 2.8.00. Located at: http://www.cdc.gov/phn/activities/applications-services/phnms/installation.html



Communiqués

The PHINMS Team responds to user's communiqués. Send questions, suggestions, and/or comments concerning PHINMS support or documentation to the PHINMS website using the Contact PHINMS email link located at the top of the home page.

2.0 INSTALLATION REQUIREMENTS

2.1 PHINMS 2.8.01 Tests

PHINMS 2.8.01 has been **tested** on the following:

- Operating systems:
 - Windows 2003 Server (Standard or Enterprise) SP2,
 - Windows XP SP3,
- Certified Default Database:
 - HSQL DB 1.8.0.4
 - Production Qualified Databases:
 - Microsoft SQL Server 2005,
 - MySQL 5.0,
 - Oracle 10g release 2,
 - Oracle 11g release 1,
- Application Servers:
 - Tomcat 6.0.14,
- Proxy Servers:
 - IIS 6.0 with Web logic 10.3 plug-in,
 - IIS 6.0 with Jakarta Tomcat Connector 1.2.27, and

PHINMS has tested the Java Database Connectivity (JDBC) drivers to connect to the supported databases shown in Table 1. Based on the tests performed, no issues were found. PHINMS does not guarantee nor support the JDBC drivers shown below. It is up to the PHINMS customer to decide which JDBC driver to use. The table is provided for reference purposes only.

DB SERVER	VERSION	JDBC DRIVER NAME	TYPE	VERSION	DATE
MS SQL	2005	sqljdbc.jar	4	1.2.2828	10/11/2007
MS SQL	2008	Sqljdbc4.jar	4	2.0	03/25/2009
Oracle	10g Rel 2	ojdbc14.jar	4	10.2.0.2	01/22/2006
Oracle	11g Rel 1	ojdbc6.jar	4	11.1.0.7.0	08/28/2008
MySQL	5.0.67	mysql-connector-java-5.1.6-bin.jar	4	3.51.27	11/20/2008

Table 1. JDBC Drivers

2.2 System Requirements

The installation of PHINMS 2.8.01 system requirements are as follows:

- Windows 2003 SP2, Windows XP SP3,
- 512MB of disk space,
- 1GB of memory,

-
- local administrator privileges, and
 - System administrator privileges on Windows

Ensure all the correct ports, which may be 5088 (default local host port), 443 (Secure Socket Layer (SSL) - Hyper Text Transfer Protocol over Secure Sockets Layer (HTTPS)), and 389 (Lightweight Directory Access Protocol (LDAP)) are open on the firewall.

Once the requirements above have been met, proceed to Section 2.3. Section 2.3 and Section 2.4 can be accomplished simultaneously.

2.3 Apply for a digital certificate:

When requesting a Digital Certificate Go to <http://ca.cdc.gov> and enroll in Secure Data Network. The Enrollment password is provided by the PHIN Helpdesk. Contact the PHIN helpdesk at 1-800-532-9929, to obtain a password and assistance applying for Digital Certificate. Refer to the information below to apply for the SDN PHINMS Program and Activity:

SDN PHINMS Digital Certificate Activities

Staging	Program = "Test"	Activity = "PHINMS 2.0"
Production	Program = "Public Health Information Network"	Activity = "PHINMS 2.0"

2.4 Request PartyID

A PartyID is required for each organization and every organization sending and receiving messages to the CDC. A PartyID uniquely identifies a PHINMS installation, also called an instance or node. The PartyID is included with every message informing the recipient of the originator.

The PHINMS Help Desk provides the PartyID. The PartyID value must be the same as the Message Receiver's PartyID in the Collaboration Protocol Agreement.

To obtain the PHINMS software, contact the PHIN Help Desk. Information will be required about the organization(s) sending and receiving messages. When complete, the Public Health Information Network (PHIN) Help Desk will email the PartyID to the requestor. Contact the PHIN Help Desk regarding any issues encountered with the PartyID, by sending an email to PHINTech@cdc.gov.

Setting up the PHINMS software requires the PartyID which is permanent and not required to be stored for later use. The PartyID is stored as long as the PHINMS instance for sending messages to partners is being used by the PHINMS application. The PHINMS application will need to be reinstalled if the PartyID needs to be changed.



Note: When a need to install PHINMS at more than one site or to install more than one PHINMS installation at the same site, a PartyID is required for each installation.

The recommended way to install PHINMS 2.8.01 is to download the application from the File Transport Site (FTP) site.

3.0 DOWNLOAD & INSTALL THE PHINMS SOFTWARE

Install the PHINMS 2.8.01 following the steps below:

Note: Refer to Section 2.4 if an email was not received with the PartyID information.

1. Navigate to <ftp://sftp.cdc.gov> displaying Figure 3.1,



Figure 3.1. Log On As

2. Enter User name, Password, select LogOn displaying Figure 3.2,

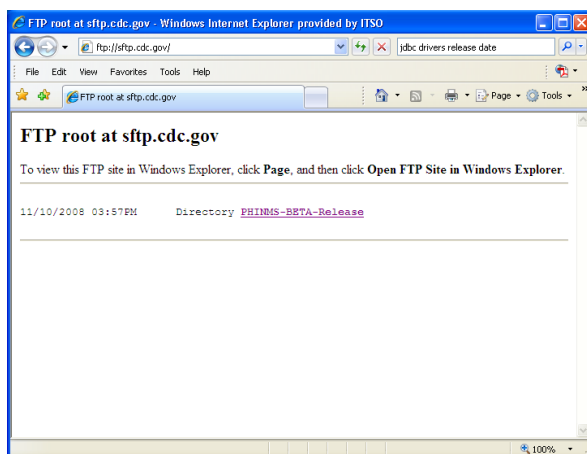


Figure 3.2. Phinms2.8.01 FTP downloads

3. To view this FTP site in Windows Explorer, click Page, and then click Open FTP Site in Windows Explorer, displaying Figure 3.3,

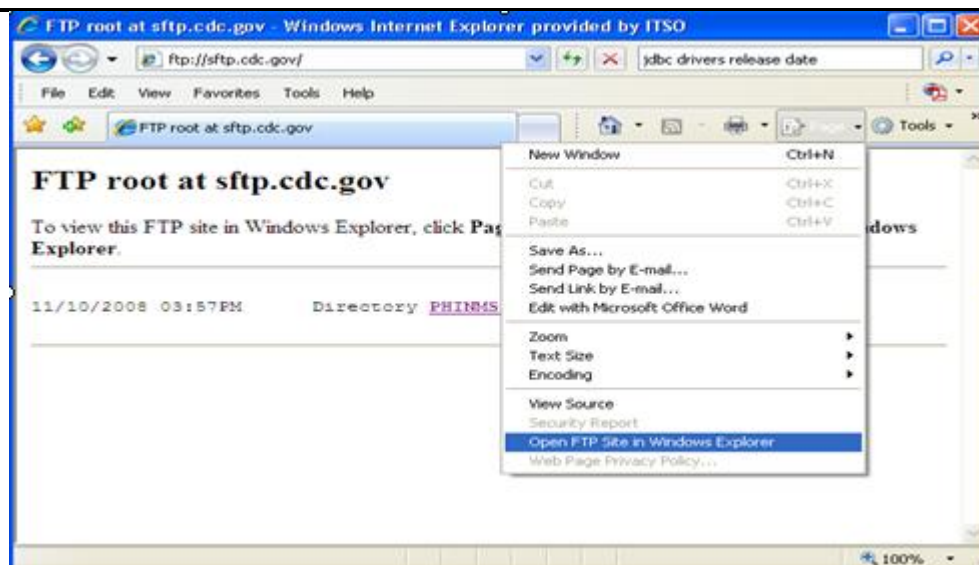


Figure 3.3. Phinms2.8.01 open FTP site in Windows explorer

4. Enter User name, Password, select LogOn displaying Figure 3.4,



Figure 3.4. Phinms2.8.01 FTP downloads windows explorer view

5. Navigate through the windows explore directory structure for the FTP site displaying Figure 3.5,

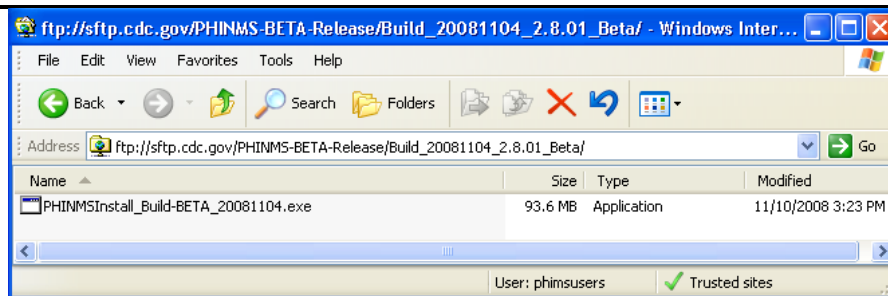


Figure 3.5. Phinms2.8.01 FTP Windows Build

6. Double-click on PHINMS2.8.01.GA.20081210.exe file displaying Figure 3.6

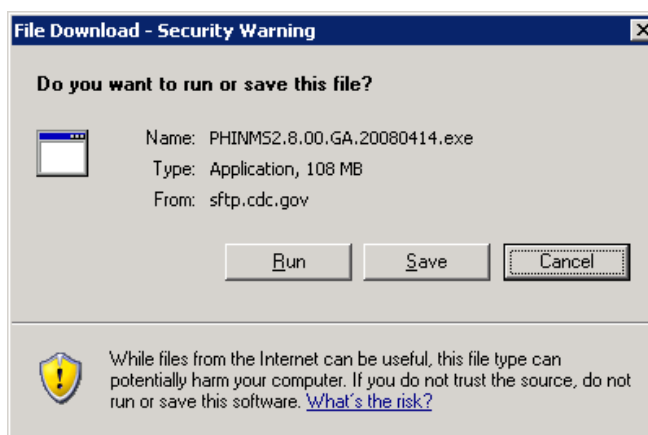


Figure 3.6. File Download - Security Warning

7. Select Save, to save the application to your local computer and double-click Phinms2.8.01.GA.20081211.exe displaying Figure 3.7,

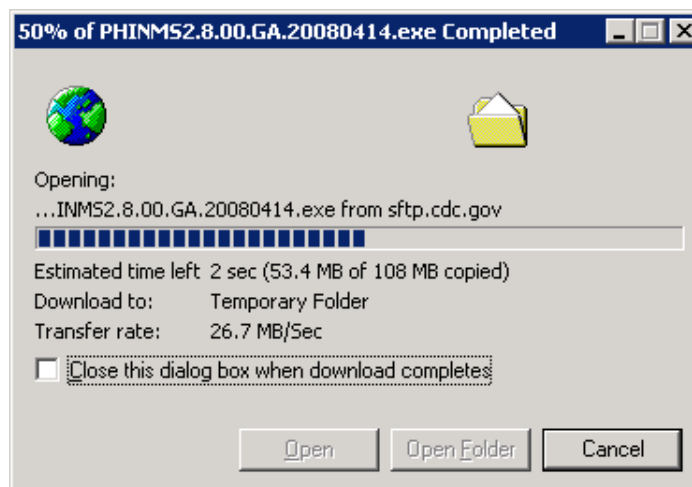


Figure 3.7. Opening PHINMS 2.8.01

Note: The Install Wizard will take a few moments displaying in Figure 3.8,

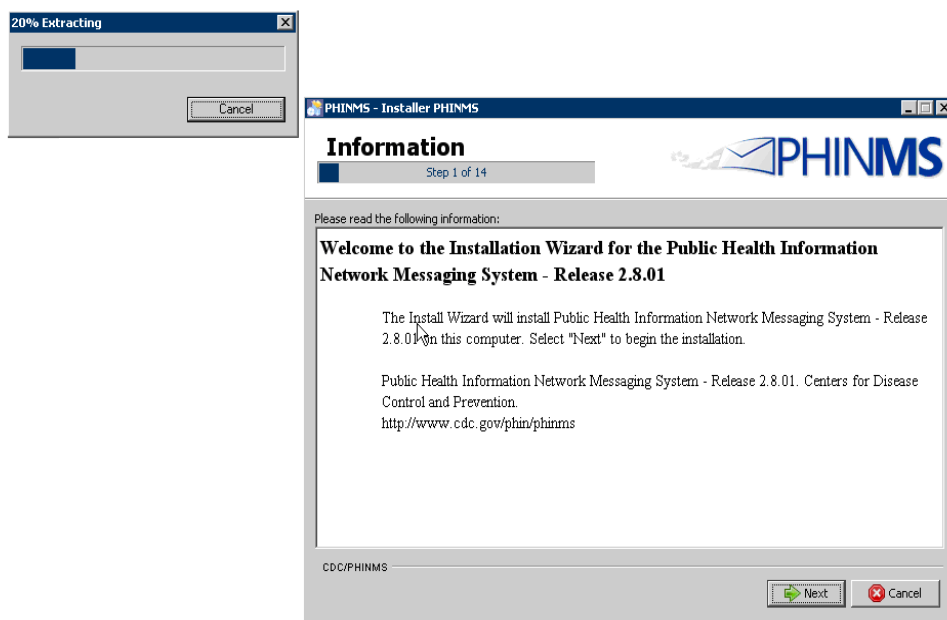


Figure 3.8. Install Shield Wizard Preparation Screens

8. Select Next displaying Figure 3.9,

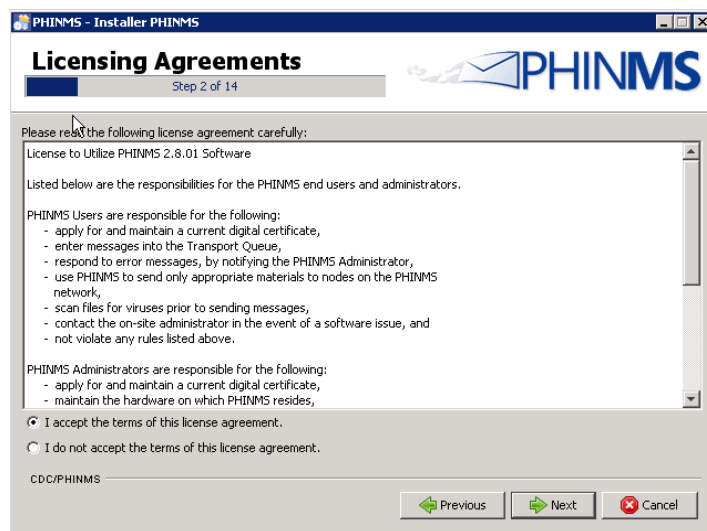


Figure 3.9. End User Agreement Screen

9. Select I accept the terms of the license agreement, select Next displaying Figure 3.10,

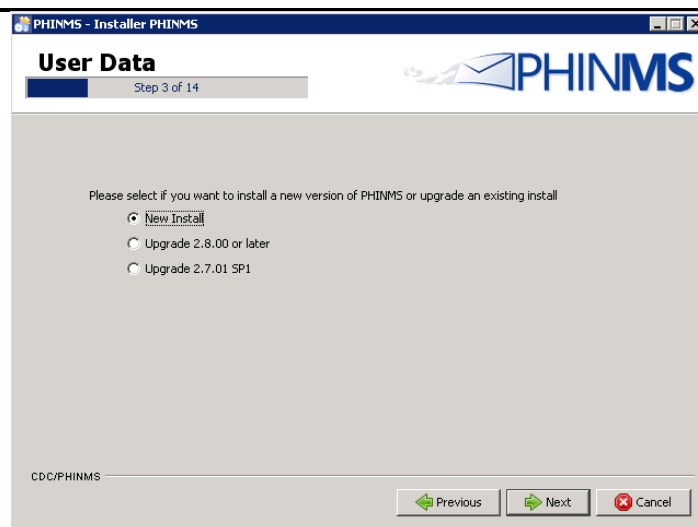


Figure 3.10. New Installation or Upgrade Screen

10. Select New PHINMS Installation, select Next displaying Figure 3.11,

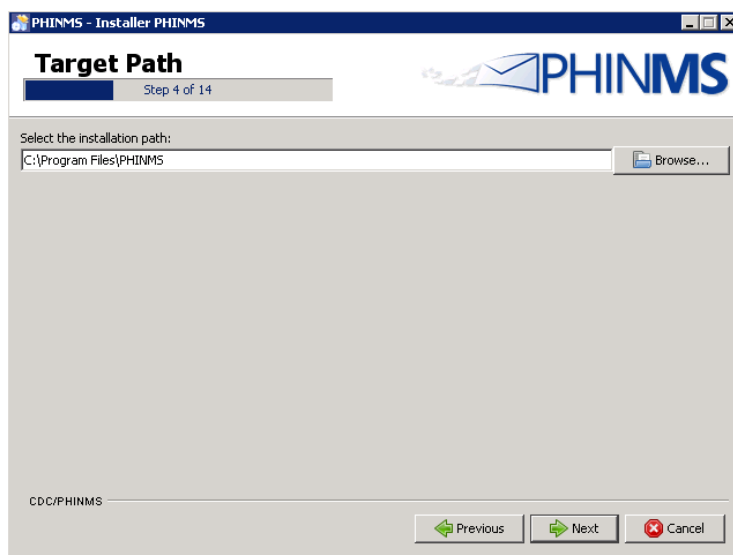


Figure 3.11. Directory Name Screen

11. Select Browse to install to a different directory or Next displaying Figure 3.12,

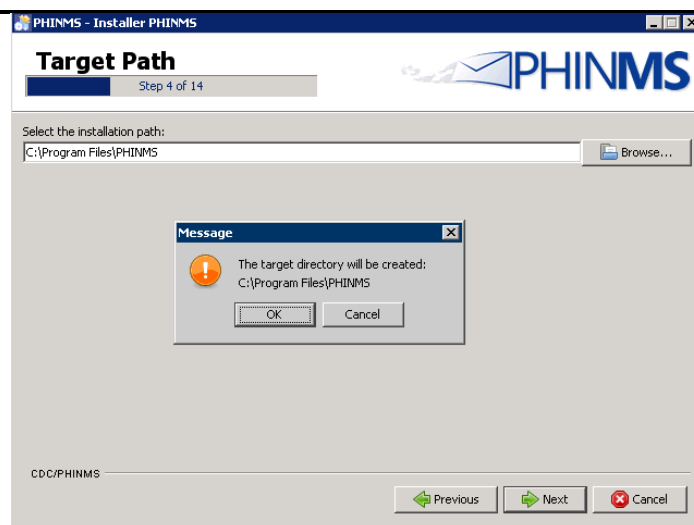


Figure 3.12. The target directory will be created

12. Select ok to create the target directory or cancel to change directory, select next to continue to displaying Figure 3.13,

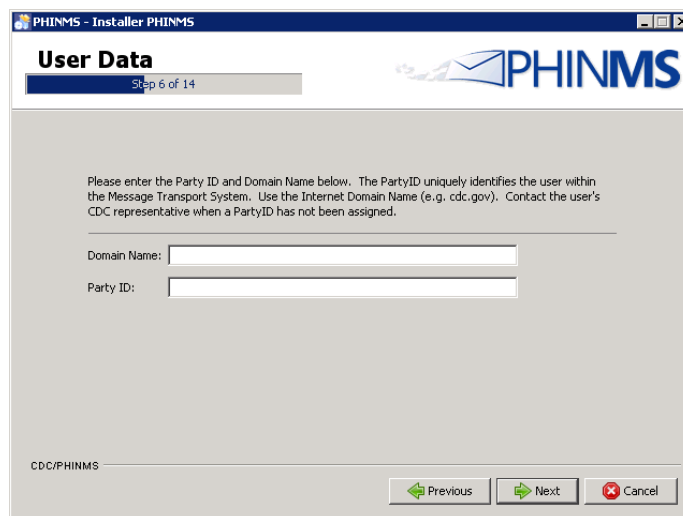
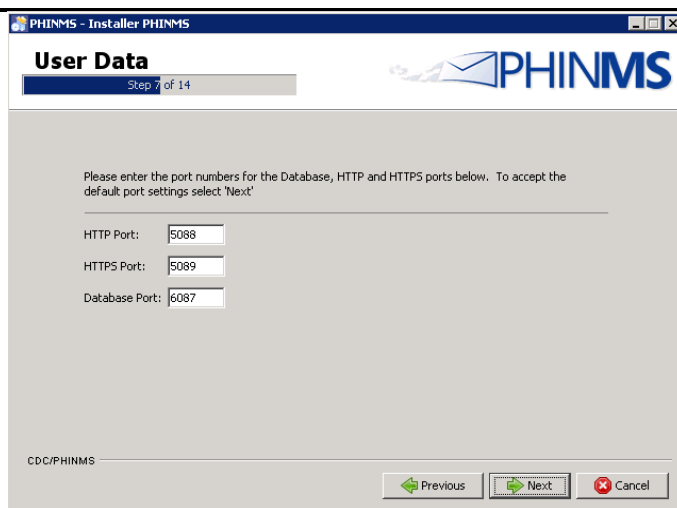


Figure 3.13. PartyID and Domain Name Screen

13. Enter the PartyID and Domain Name, select Next displaying Figure 3.14,



PHINMS - Installer PHINMS

User Data
Step 7 of 14

Please enter the port numbers for the Database, HTTP and HTTPS ports below. To accept the default port settings select 'Next'

HTTP Port:

HTTPS Port:

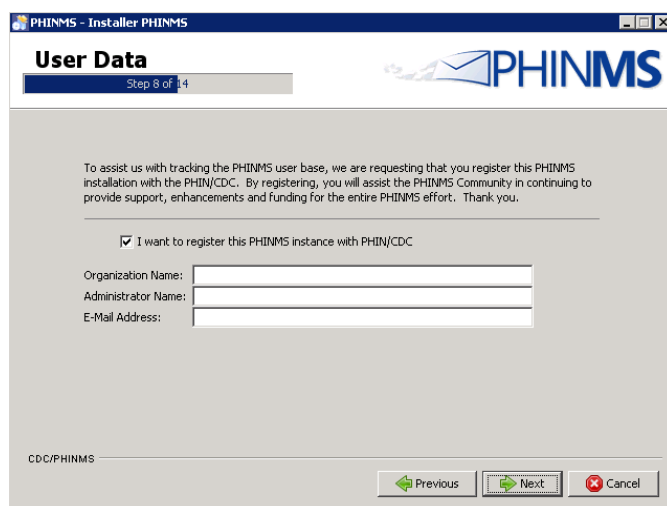
Database Port:

CDC/PHINMS

Figure 3.14. Port Numbers Screen

Note: The PHINMS default port numbers are 6087 for the Database, 5088 for HTTP, and 5089 for HTTPS.

14. Select Next displaying Figure 3.15 then the registration screen displays, It is optional to enter Business/Organization Name, Name, Email to register the product with the CDC,



PHINMS - Installer PHINMS

User Data
Step 8 of 14

To assist us with tracking the PHINMS user base, we are requesting that you register this PHINMS installation with the PHIN/CDC. By registering, you will assist the PHINMS Community in continuing to provide support, enhancements and funding for the entire PHINMS effort. Thank you.

☒ I want to register this PHINMS instance with PHIN/CDC

Organization Name:

Administrator Name:

E-Mail Address:

CDC/PHINMS

Figure 3.15. Register this PHINMS instance with PHIN/CDC

15. Select Next displaying Figure 3.16 then the Installation Package screen,

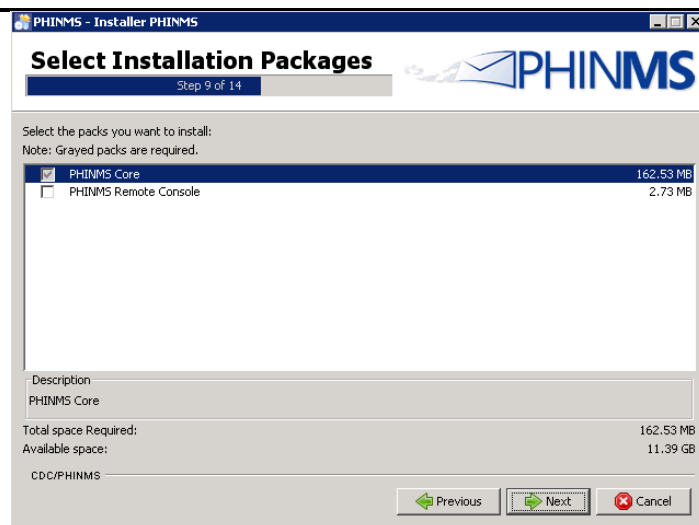


Figure 3.16. Installation Package screen

16. Select Next displaying Figure 3.17,

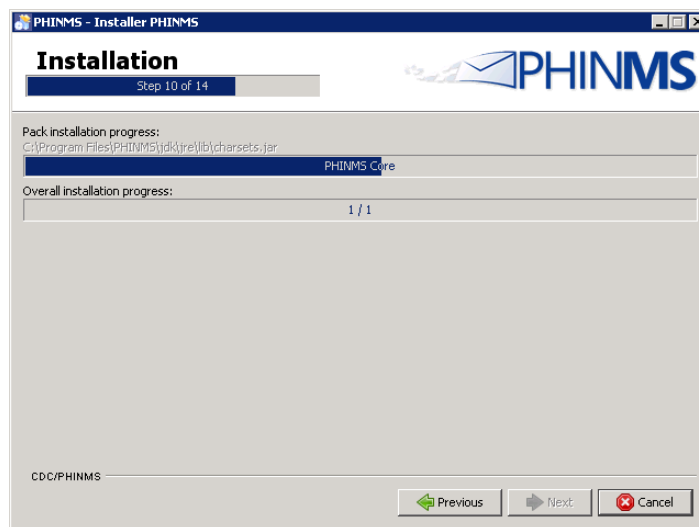


Figure 3.17. Installation

17. Select Next displaying Figure 3.18,

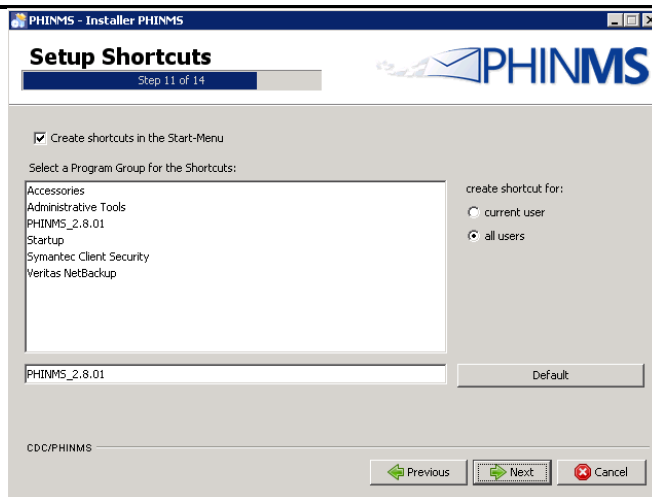


Figure 3.18. Setup Shortcuts

Note: Select where the shortcut should be created, if you choose to relocate the shortcut while on this screen after your first choice has been made, choose default to reset this screen.

18. Select Next displaying Figure 3.19.

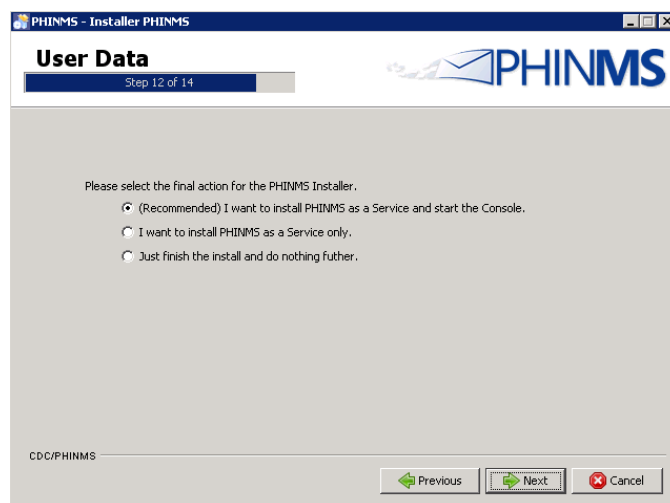


Figure 3.19. PHINMS Installation Options

19. Select how PHINMS is to be installed (i.e., as a Service and start Console, Service only, or not as a Service). Select Next displaying Figure 3.20.

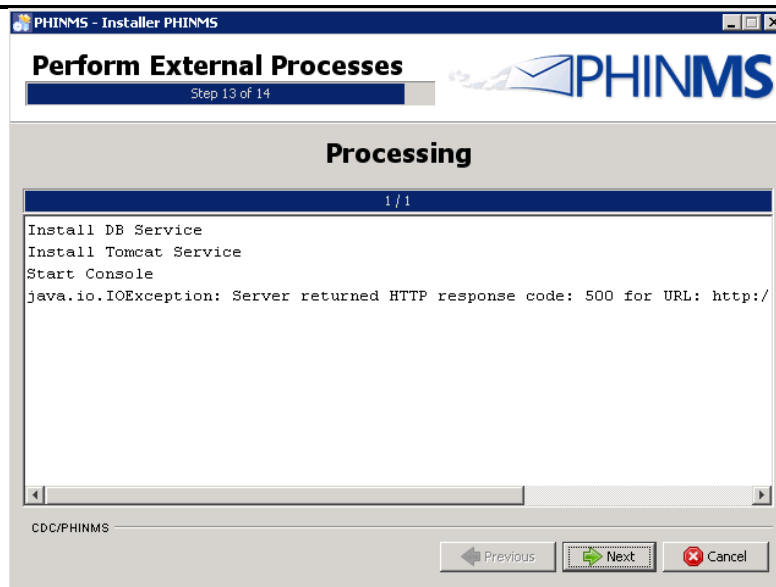


Figure 3.20. PHINMS Processing

20. Select Next displaying Figure 3.21.

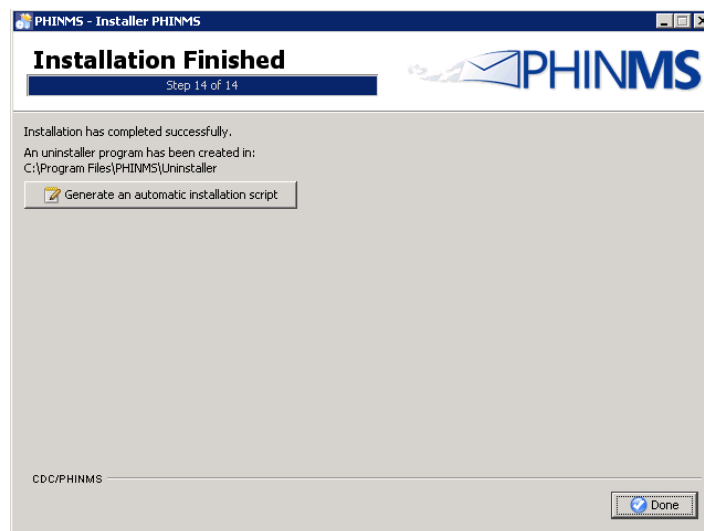


Figure 3.21. PHINMS Installation Finished

Note: Your installation has been completed successfully. An uninstaller has been created. You have an option to generate an automatic installation script to deploy PHINMS with the same configuration on another system.

21. Select Done to initiate PHINMS for the first time, displaying Figure 3.22.

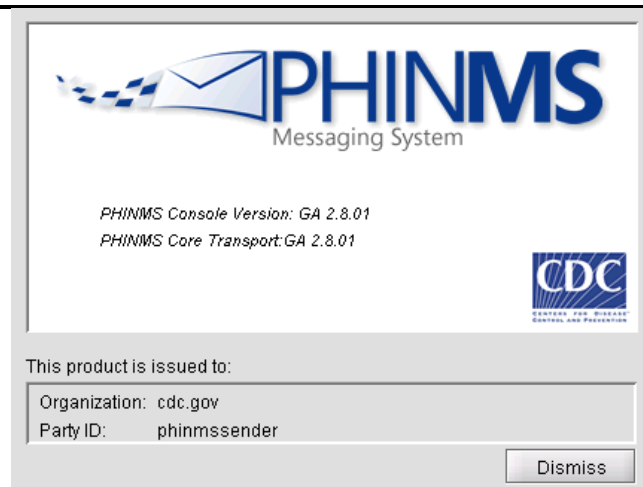


Figure 3.22. PHINMS Welcome screen

22. Please wait while the PHINMS Console login screen comes up, displaying Figure 3.23.

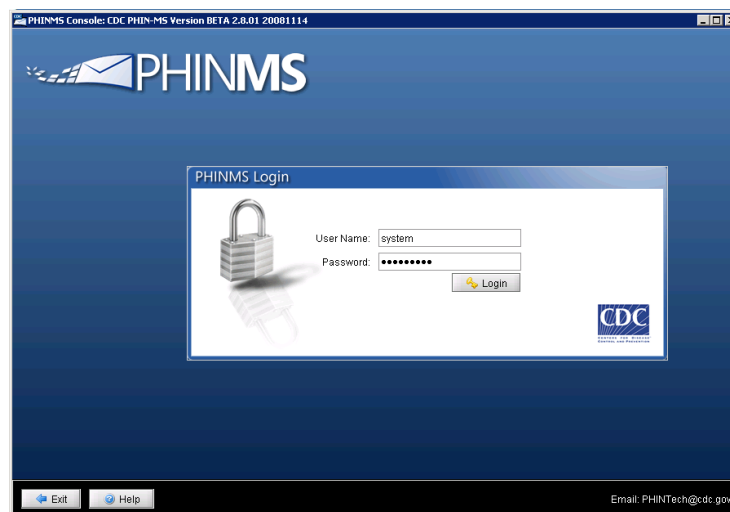


Figure 3.23. PHINMS Console Login Screen

23. Enter Username and Password the click Login, displaying Figure 3.24.

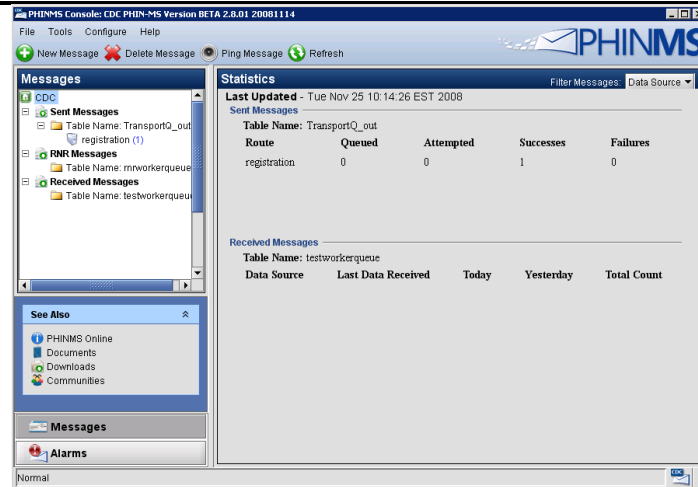


Figure 3.24. PHINMS Console

4.0 UPGRADE PHINMS SOFTWARE

PHINMS 2.8.01 allows the user to upgrade from version 2.7.00 SP1 and PHINMS 2.8.00 only. Prior versions of the PHINMS software will be required to upgrade to version 2.7.00 SP1 before upgrading to version 2.8.01.

Note: The PHINMS upgrade will not overwrite the previous 2.7.00 SP1 version. It will install PHINMS 2.8.01 in a new location and pull the configuration files, mainly the TransportQ table configuration information and use this information to configure the new PHINMS 2.8.01 application. This allows the user to have the previous installation intact if there are any problems.

Complete the following steps to upgrade to version 2.8.01 from version 2.7.00 SP1:

Open the executable file PHINMS2.8.01.GA.20081210.exe displaying Figure 4.1, the Install Wizard will take a few moments displaying in Figure 4.1,

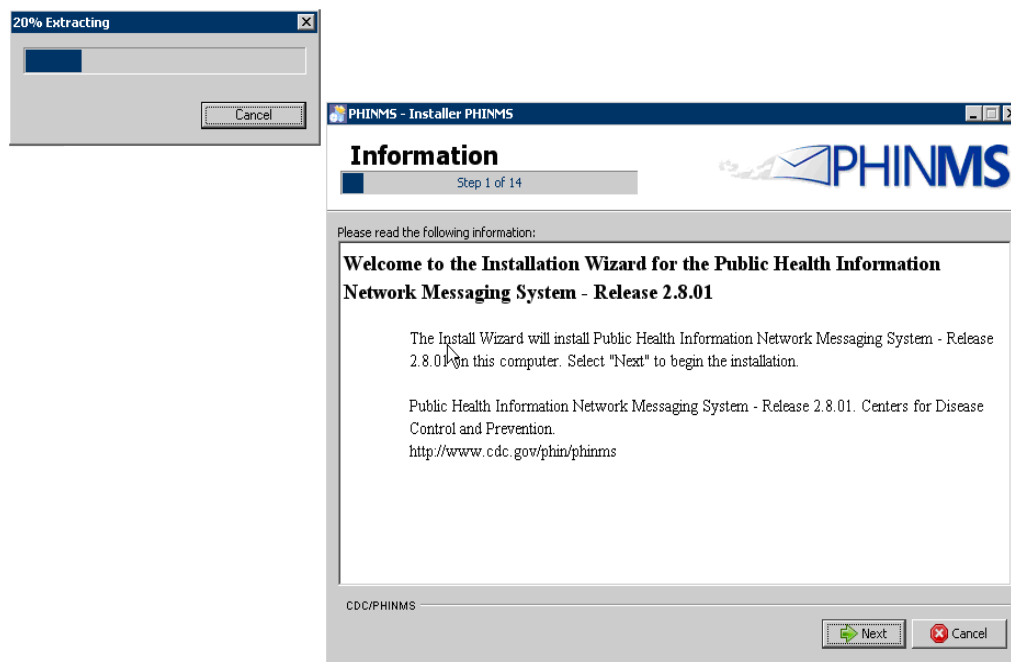


Figure 4.1. Install Shield Wizard Preparation Screens

Select Next displaying Figure 4.2,

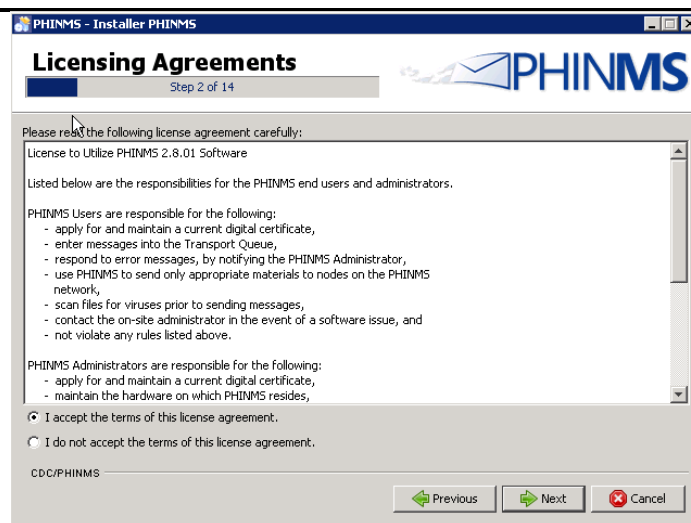


Figure 4.2. End User Agreement Screen

3. Select I accept the terms of the license agreement,
4. Select Next displaying Figure 4.3,

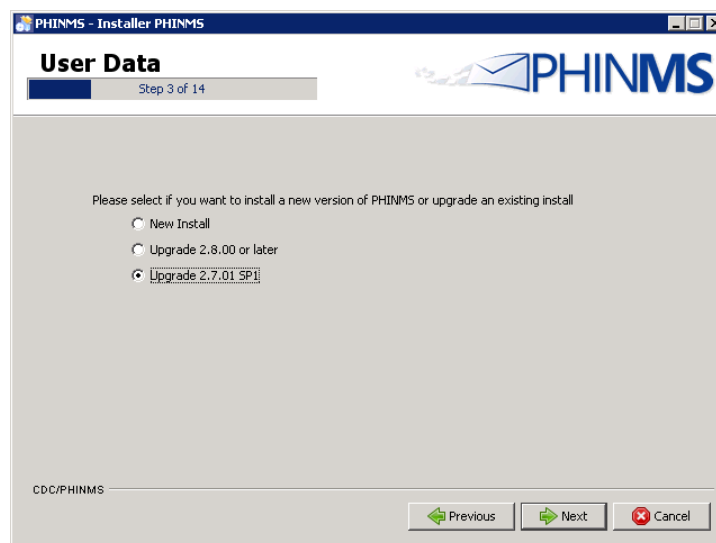


Figure 4.3. New Installation or Upgrade Screen

5. Select Upgrade PHINMS Software, Next displaying Figure 4.4,

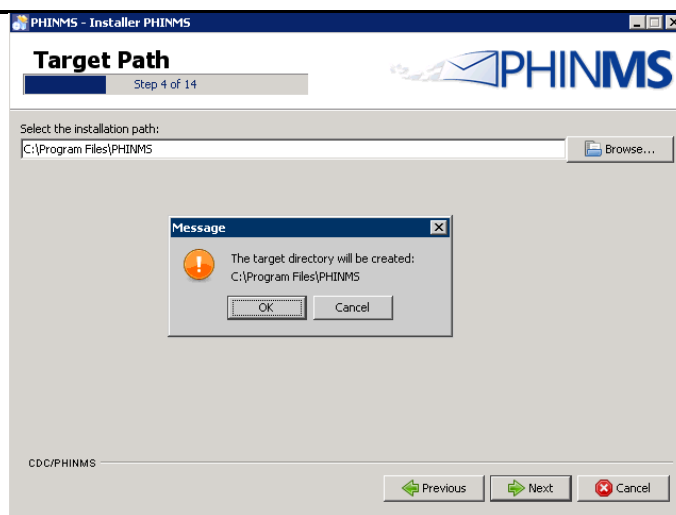


Figure 4.4. The target directory will be created

6. Select ok to create the target directory or cancel to change directory, Select next to continue to displaying Figure 4.5

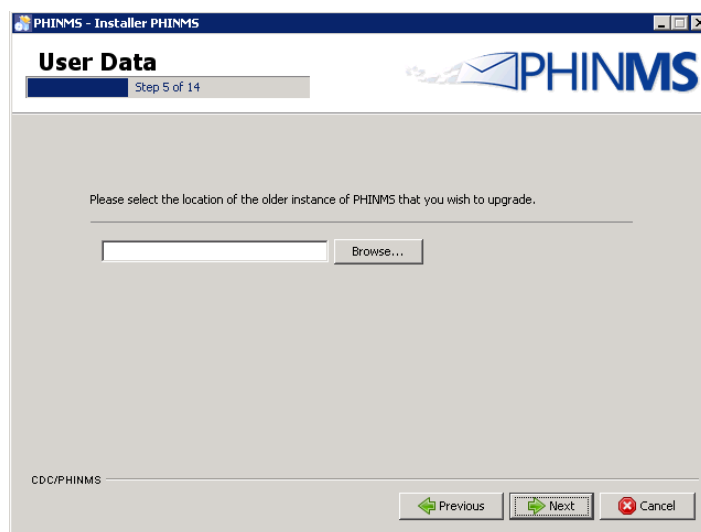


Figure 4.5. The PHINMS 2.7.00 SP1 directory path

Note: The upgrade location is where the PHINMS 2.7.00 SP1 is stored. Select Browse to change the location if not accurately populated.

7. Enter directory path for the PINMS Instance to be Upgraded, Select next to continue to displaying Figure 4.6

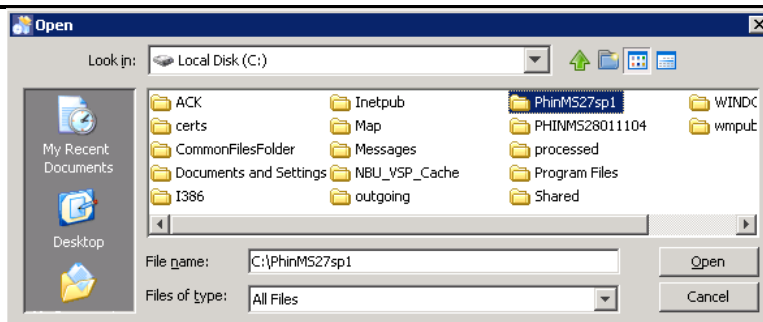


Figure 4.6. The PHINMS 2.7.00 SP1 directory path

8. Point to the PHINMS directory path for the PHINMS Instance to be Upgraded, Select open to continue to displaying Figure 4.7

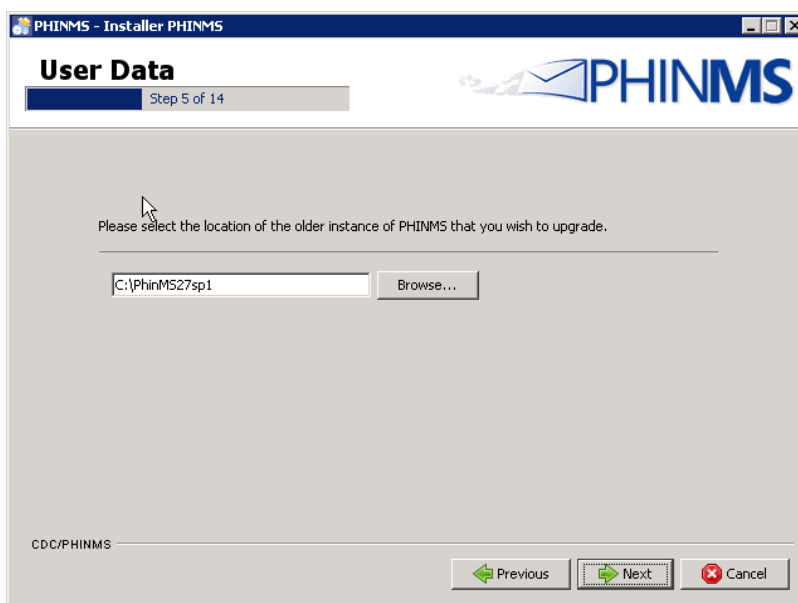


Figure 4.7. Upgrade Location

9. Select Next displaying Figure 4.8,

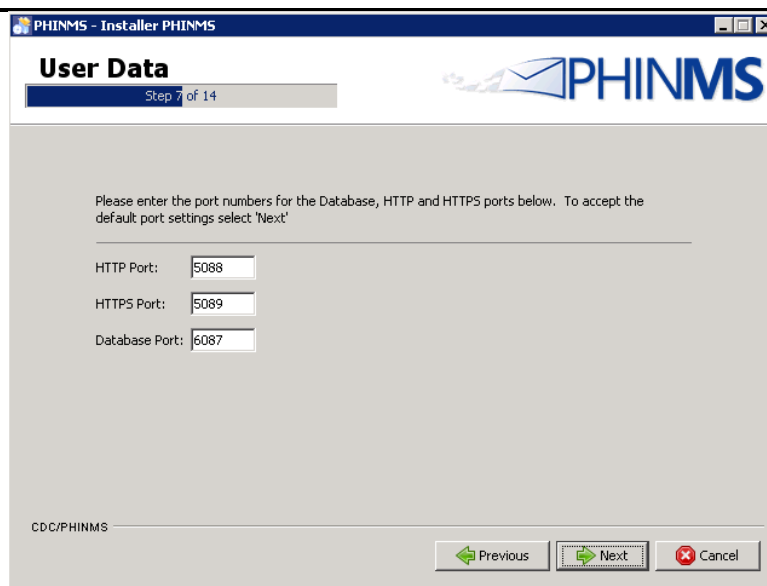


Figure 4.8. Port Numbers Screen

Note: The PHINMS default port numbers are 6087 for the Database, 5088 for HTTP, and 5089 for HTTPS.

10. Select Next displaying Figure 4.9 then the Installation Package screen,

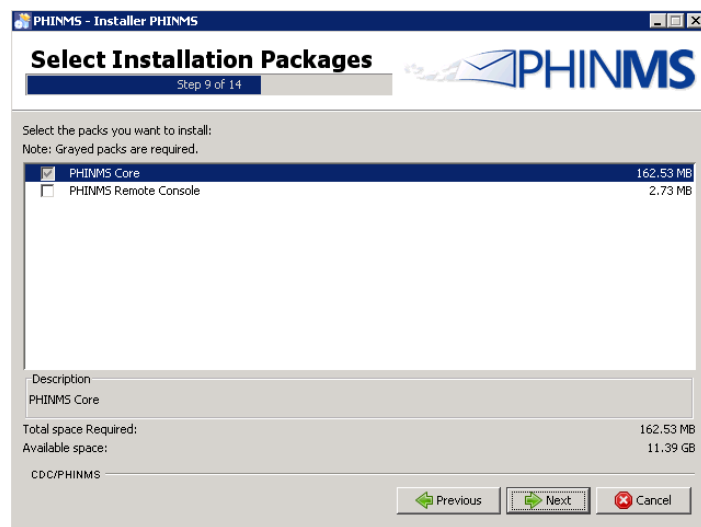


Figure 4.9. Installation Package screen

11. Select Next displaying Figure 4.10,

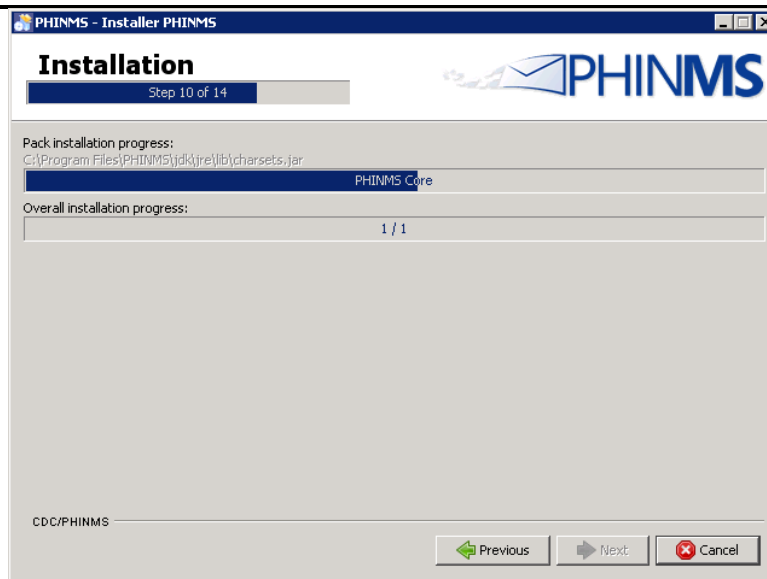


Figure 4.10. Installation

12. Select Next displaying Figure 4.11,

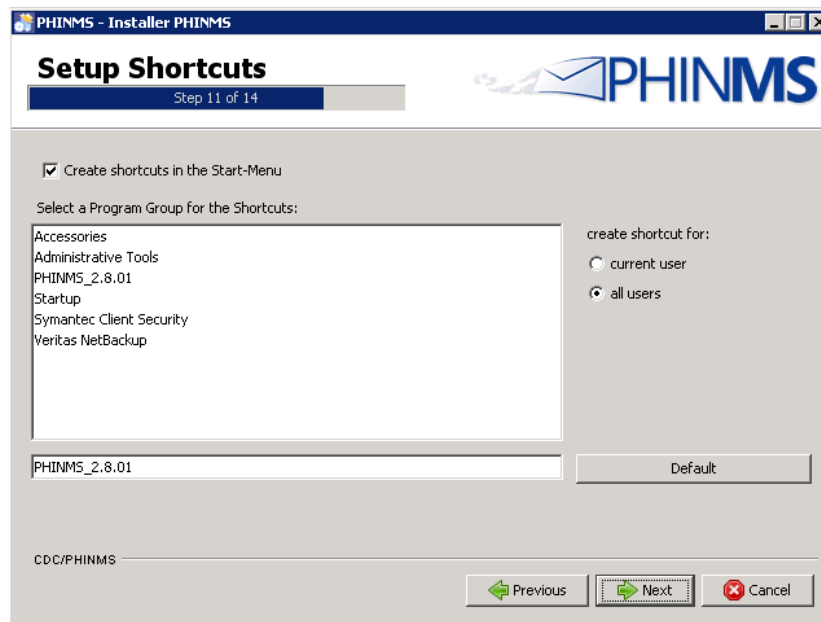


Figure 4.11. Setup Shortcuts

Select where the shortcut should be created, if you choose to relocate the shortcut while on this screen after your first choice has been made, choose default to reset this screen.

13. Select Next displaying Figure 4.12.

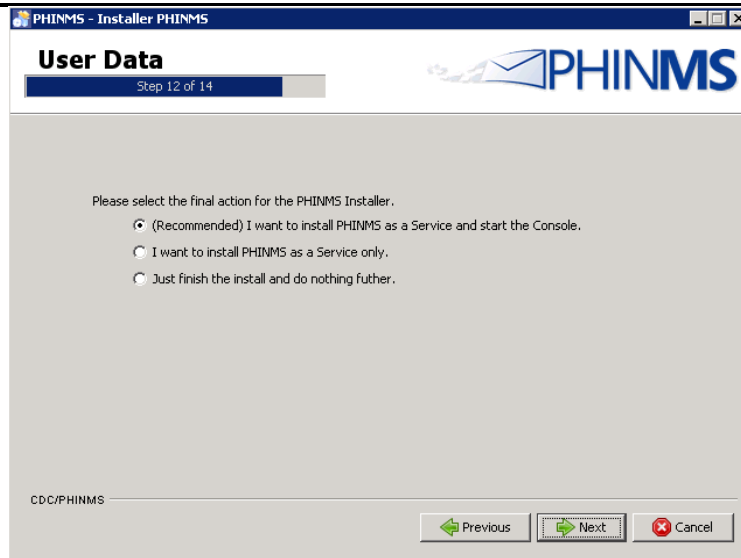


Figure 4.12. PHINMS Installation Options

14. Select how PHINMS is to be installed (i.e., as a Service and start Console, Service only, or not as a Service). Select Next displaying Figure 4.13.

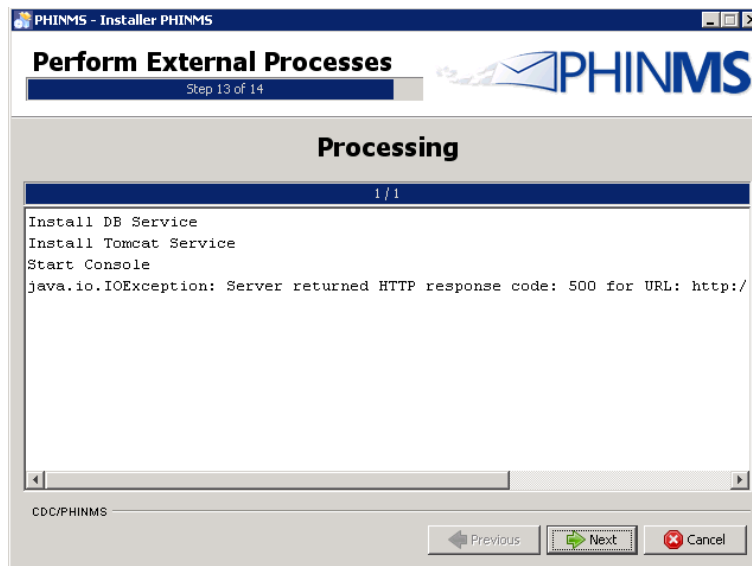


Figure 4.13. PHINMS Processing

15. Select Next displaying Figure 4.15.

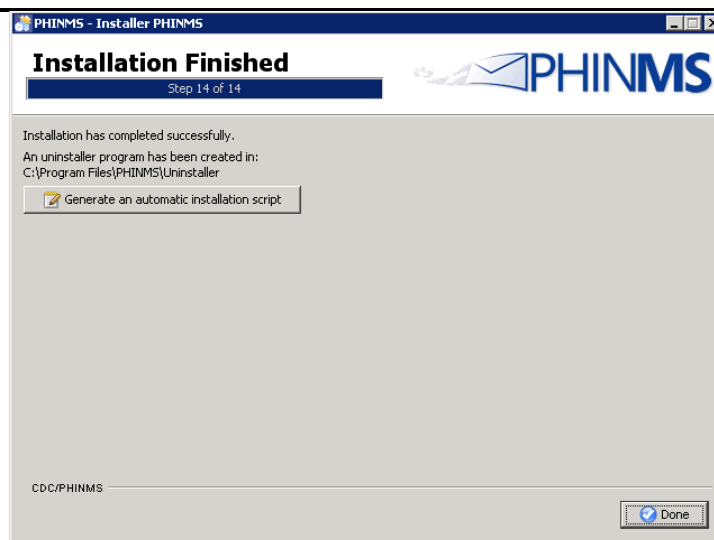


Figure 4.15. PHINMS Installation Finished

Notes: Your installation has been completed successfully. An uninstaller has been created. You have an option to generate an automatic installation script to deploy PHINMS with the same configuration on another system.

16. Select done to initiate PHINMS for the first time, displaying Figure 4.16.

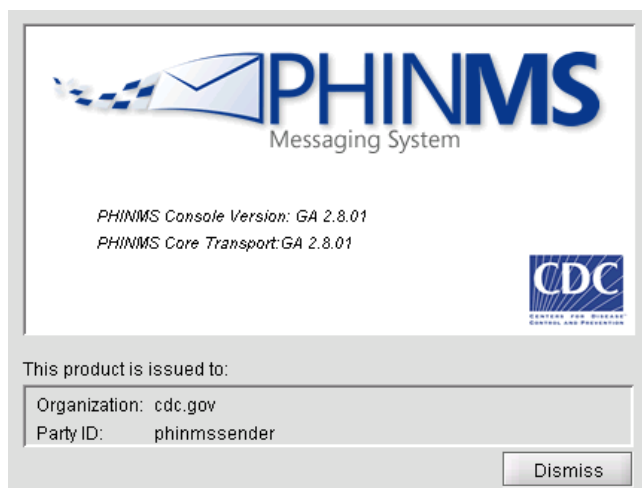


Figure 4.16. PHINMS Welcome screen

17. Please wait while the PHINMS Console login screen comes up, displaying Figure 4.17.



Figure 4.17. PHINMS Console Login Screen

18. Enter Username and Password the click Login, displaying Figure 4.18.

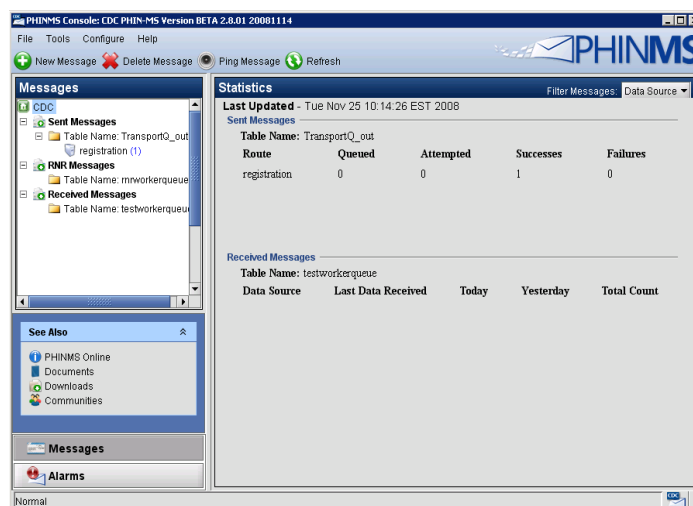


Figure 4.18. PHINMS Console

5.0 CONFIGURE SQL DATABASES

A Structured Query Language (SQL) database containing a Transport Queue (TransportQ) is automatically installed with the PHINMS 2.8.01 application. An external database can be created for the purpose of hosting the messaging queue tables. PHINMS 2.8.01 will support the following databases for hosting messaging queues:

- HSQLDB 1.8.0.
- Microsoft SQL Server 2005,
- MySQL 5.0,
- Oracle 10g and 11g.

A HSQL database is provided with the PHINMS installation on the Windows platform as a default database and facilitates testing installation. Evaluation of the tradeoffs between SQL and a high transaction volume Relational Database Management System (RDBMS) such as others listed above is recommended.

All Table scripts needed for PHINMS external database configurations for the databases listed above will be posted on the FTP site (<ftp://sftp.cdc.gov>). The provided table scripts are for the Transport Queue, Worker Queue only.

6.0 SENDER INFORMATION

PHINMS Version 2.8.01 installation has two components - the Sender and the Receiver. Sending a test message allows the PHINMS Sender to send messages to the TransportQ and to the CDC. Testing the PHINMS installation is a three-part procedure which includes the following:

- ping the PHINMS Sender loopback route,
- ping the PHINMS CDC Ping Server (phinmsping.cdc.gov), and
- ping the PHINMS CDC Staging Receiver. (Requires Collaboration Protocol Agreement (CPA) files be emailed to Phintech@cdc.gov. Refer to Section 6.4 for more information.

Figure 6.1 displays a diagram to assist with understanding the PHINMS authentication process.

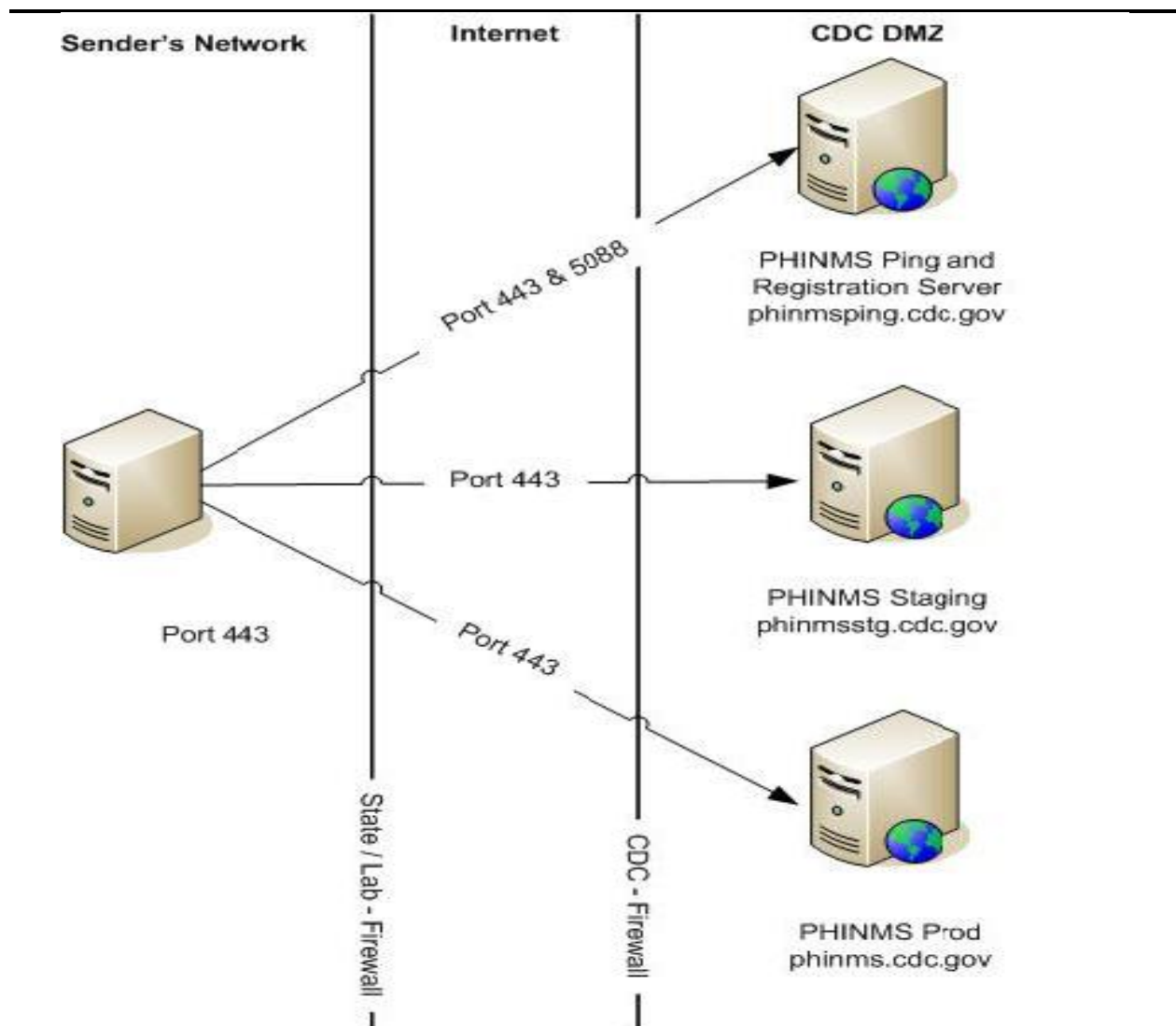


Figure 6.1. CDC PHINMS Topology

6.1 Ping Loopback

The Ping Loopback validates the PHINMS installation was downloaded and installed successfully on the Sender's system. This is not a test to verify messages can be sent outside of a firewall if one is present.

Verify the generated ping loopback is successfully sent to the loopback message processor by completing the following steps:

Open the PHINMS 2.8.01 Console displaying Figure 6.2,

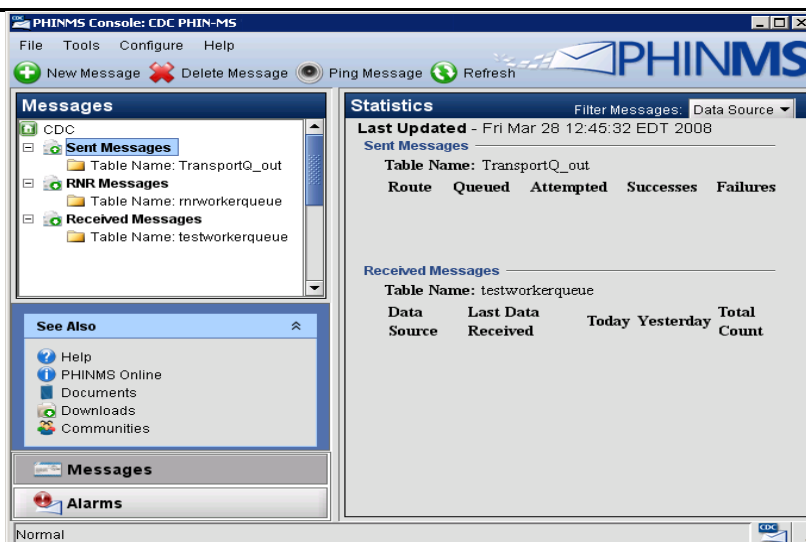


Figure 6.2. PHINMS 2.8.01 Console

Select Ping Message displaying Figure 6.3,

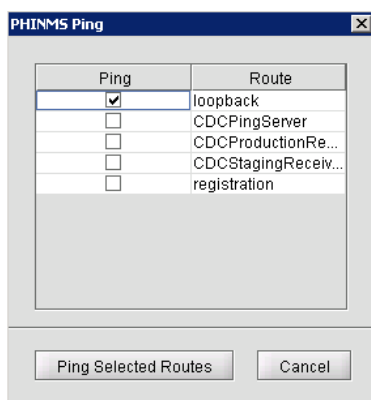


Figure 6.3. PHINMS Ping

Select loopback,

Select Ping Selected Routes displaying Figure 6.4, and

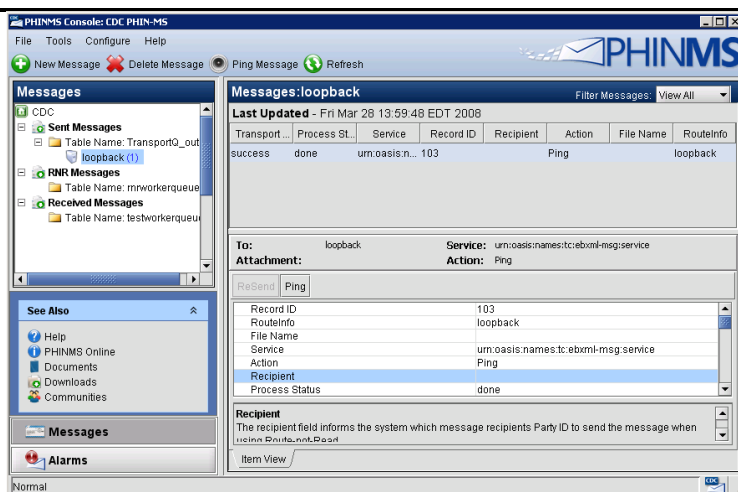


Figure 6.4. Ping Message

Select the loopback folder showing the status of the ping on the right-hand side.

Note: When the Transport Status is in the state of queued or attempted, select Refresh until the status changes.

6.2 Ping CDC Ping Server

The ping CDCPingServer validates the Sender can connect to the internet and to the CDC without the need for authentication (security credentials). The CDC Ping Server is dedicated to answering Ping requests and will not receive any real messages. Port 5088 needs to be open on the firewall at the Sender's location to generate a ping to the CDCPingServer.

Verify the message ping to the CDC Ping Server is successful by completing the following steps:

Open the PHINMS 2.8.01 Console displaying Figure 6.5,

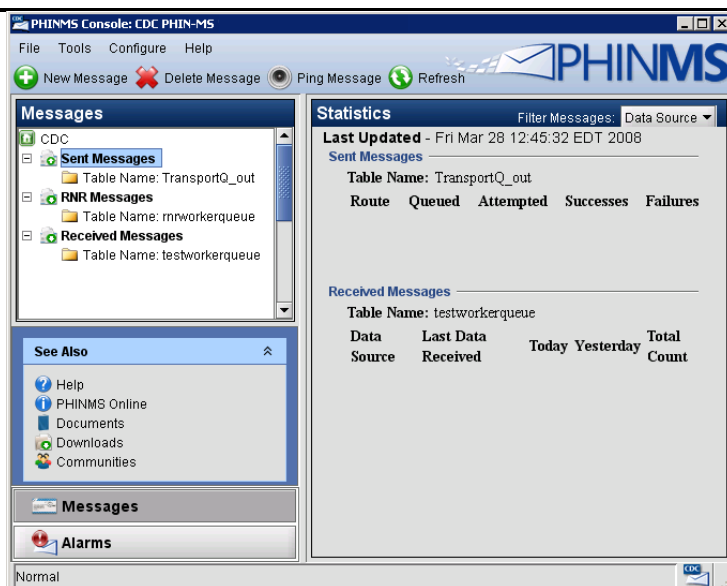


Figure 6.5. PHINMS 2.8.01 Console

Select Ping Message displaying Figure 6.6,

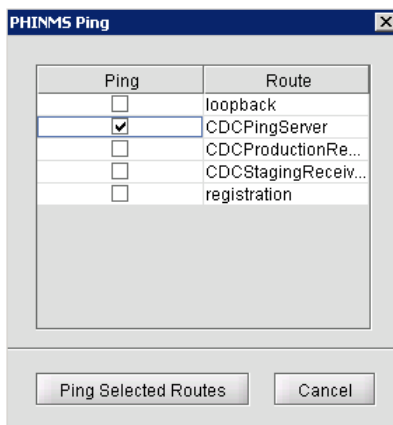


Figure 6.6. PHINMS Ping

Select CDCPingServer,

Select Ping Selected Routes displaying Figure 6.7, and

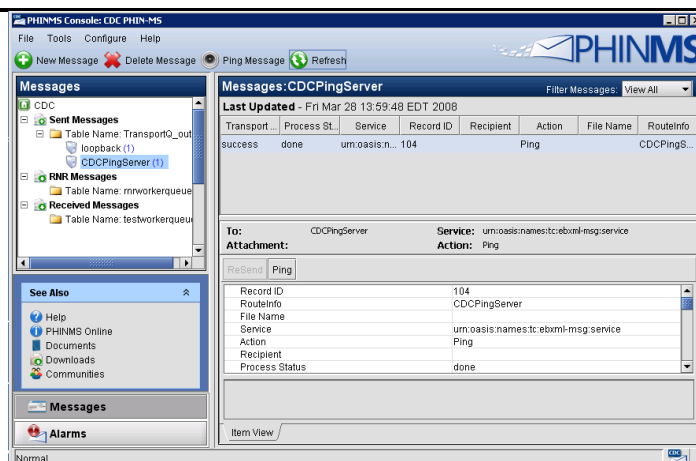


Figure 6.7. CDCPingServer Message

Select the CDCPingServer folder showing the status of the ping on the right-hand side.

Note: When the Transport Status is in the state of queued or attempted, select Refresh until the status changes.

6.3 Configure CDC Staging Receiver

The CDC Staging Receiver requires to be configured before sending a Ping. Configure the CDCStagingReceiver using the following steps:

Open the PHINMS 2.8.01 Console displaying Figure 6.8,

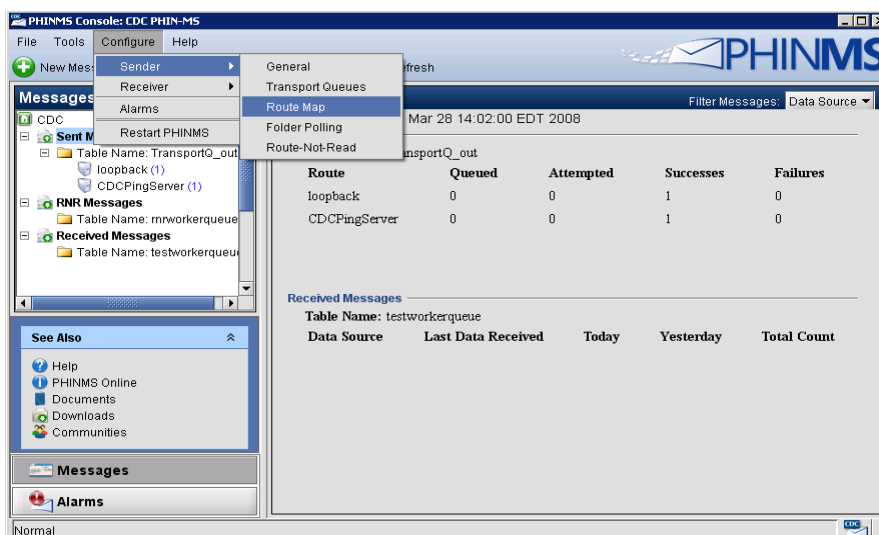


Figure 6.8. PHINMS 2.8.01 Console

Open the select Configure>Sender>Route Map displaying Figure 6.9,

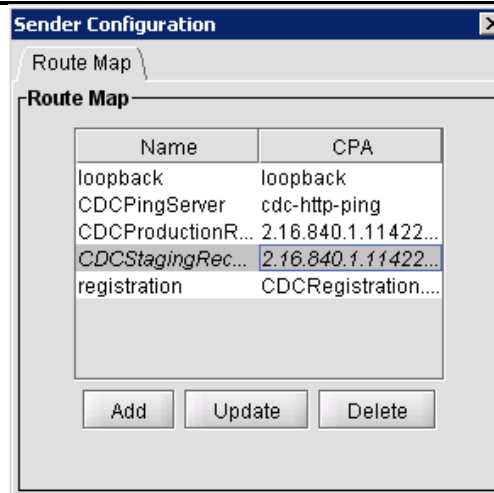


Figure 6.9. Sender Configuration

Select CDCStagingReceiver,
Select Update displaying Figure 6.10,

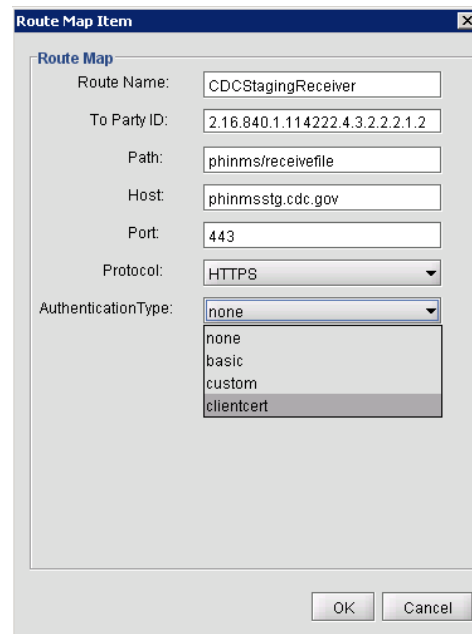
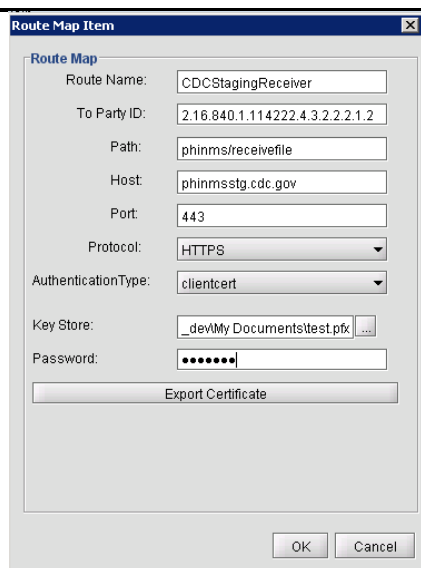


Figure 6.10. Route Map Item

Select “clientcert” from the Authentication Type dropdown list displaying Figure 6.11,



Route Map Item

Route Map

Route Name: CDCStagingReceiver

To Party ID: 2.16.840.1.114222.4.3.2.2.2.1.2

Path: phinms/receivefile

Host: phinmsstg.cdc.gov

Port: 443

Protocol: HTTPS

Authentication Type: clientcert

Key Store: _dev\My Documents\test.pfx

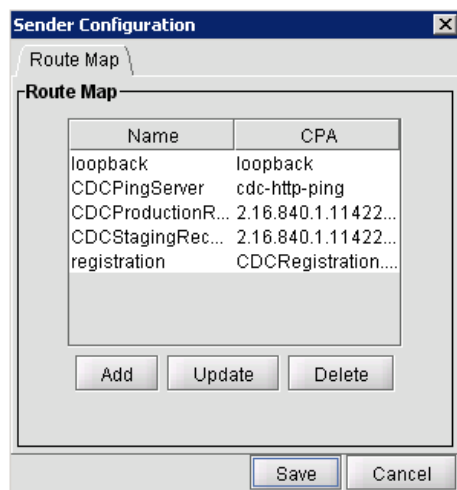
Password: *****

Export Certificate

OK Cancel

Figure 6.11. CDC Route Map Configuration

Enter the path to the stored certificate Key Store (.pfx file),
 Enter the Key Store Password in both the Key Store Password,
 Select OK, displaying Figure 6.12,



Sender Configuration

Route Map

Name	CPA
loopback	loopback
CDCPingServer	cdc-http-ping
CDCProductionR...	2.16.840.1.11422...
CDCStagingRec...	2.16.840.1.11422...
registration	CDCRegistration....

Add Update Delete

Save Cancel

Figure 6.12. CDC Route Map

Select Save, displaying Figure 6.13,

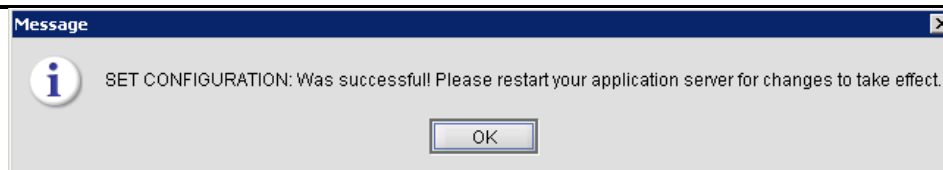


Figure 6.13. CDC Route Configuration Successful

Select OK, and
Restart PHINMS.

6.4 Email CPA File

PHINMS creates a CPA file for each route listed on the Route Map tab of the Sender Configuration panel. The PHINMS Administrator must send the PHINMS Helpdesk (Phintech@cdc.gov) the CPA files for each route specifying either the CDC Production Receiver or the CDC Staging Receiver. Only after the PHIN helpdesk has received the CPA file and applied it to the PHINMS Receiver can there be a successful transmission of messages from the Sender to the Receiver.

The CPA files required to be sent are located in directory C : \ (PHINMS install directory) \ config \ sender \ CPA.

Note: Information on CPA can be found in the PHINMS Technical Reference Guide.

6.5 Ping CDC Staging Receiver

The ping PHINMS Staging Receiver validates end-to-end success of the Sender's ability to connect to the CDC over the internet, authenticate with the CDC's Authentication Server, and communicate with the Staging Receiver.

Verify the generated ping message is successfully sent to the CDC Staging Receiver message processor by completing the following steps:

Open the PHINMS 2.8.01 Console displaying Figure 6.14,

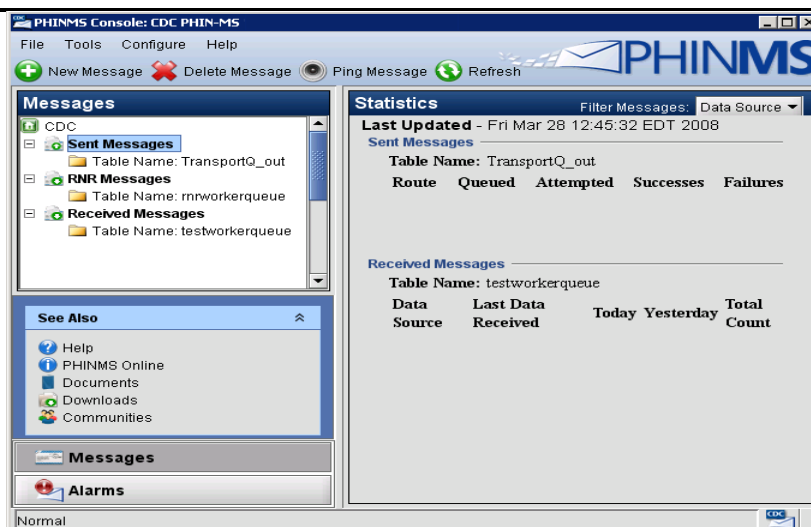


Figure 6.14. PHINMS 2.8.01 Console

Select Ping Message displaying Figure 6.15,

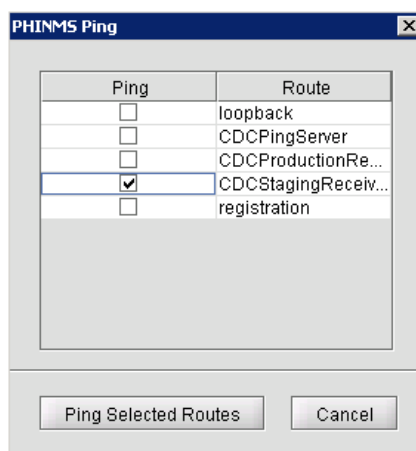


Figure 6.15. PHINMS Ping Message

Select CDCStagingReceiver,

Select Ping Selected Routes displaying Figure 6.16,

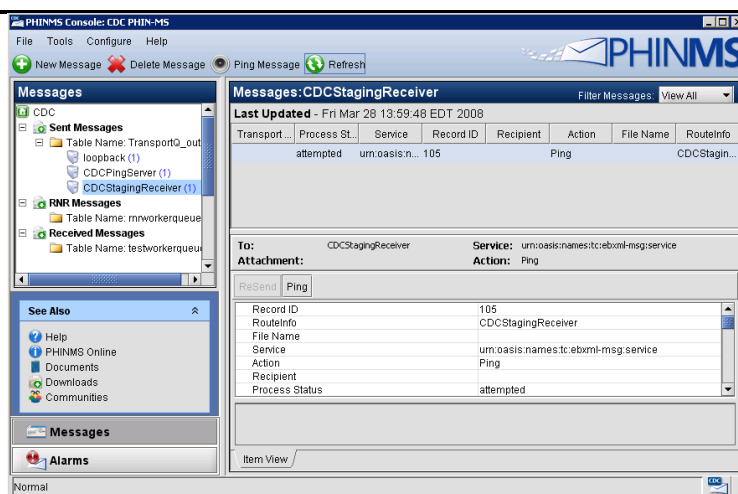


Figure 6.16. Ping Message

Select the CDCStagingReceiver folder showing the status of the ping on the right-hand side, and

Select Refresh until the status changes from queued or attempted.

6.6 Send Test Payload Message

The send payload message verifies the capability to send an outbound message with an attached file to a Receiver. Ensure the CPA files have been sent to the PHIN Help desk before attempting to send a payload message. Refer to Section 9.0 for CPA information.

Send the payload message test to the PHINMS Staging Receiver by completing the following steps:

Open the PHINMS 2.8.01 Console displaying Figure 6.17,

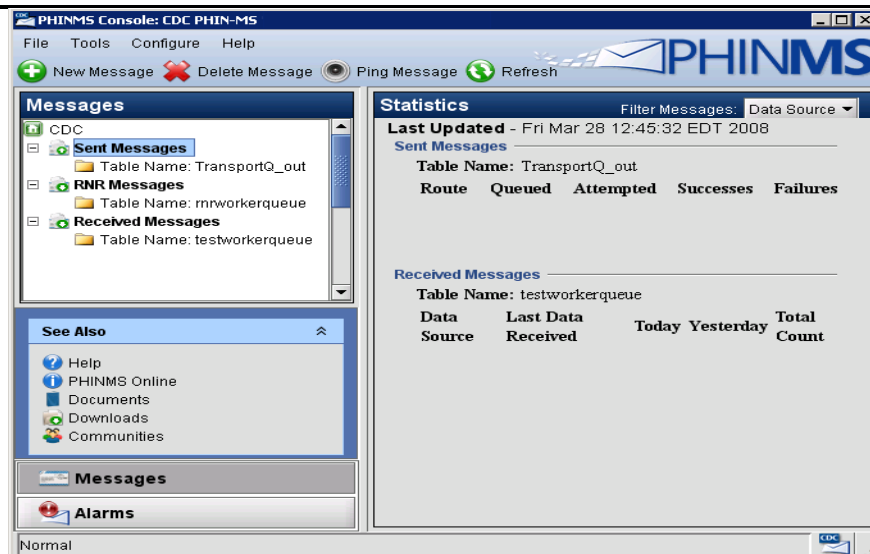


Figure 6.17. PHINMS 2.8.01 Console

Select New Message displaying Figure 6.18,

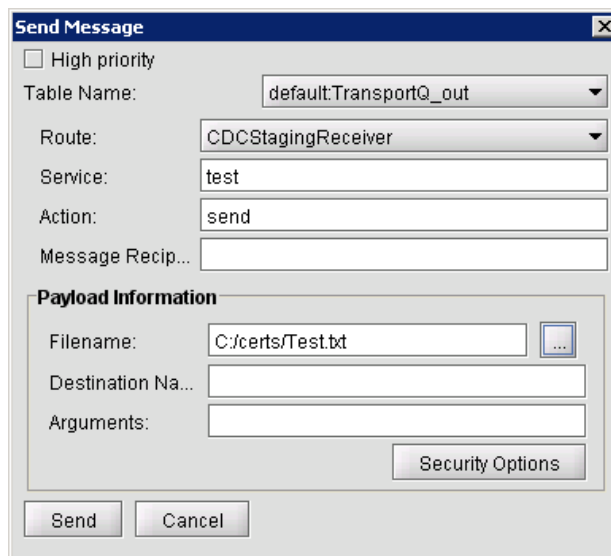


Figure 6.18. PHINMS Ping

Enter the following parameters:

- Route: CDC Staging Receiver,
- Service: **test**,
- Action: **send**,
- Message Recipient: **optional** - can be left blank,

- Filename: browse for a **file** to attach,
- Destination Name: **optional** - can be left blank,
- Arguments: **optional** - can be left blank,

Proceed to Step 5 if using Security Options and to Step 8 if not,

Note: Security Options are optional for encrypting or signing messages.

Select Security Options displaying Figure 6.19,

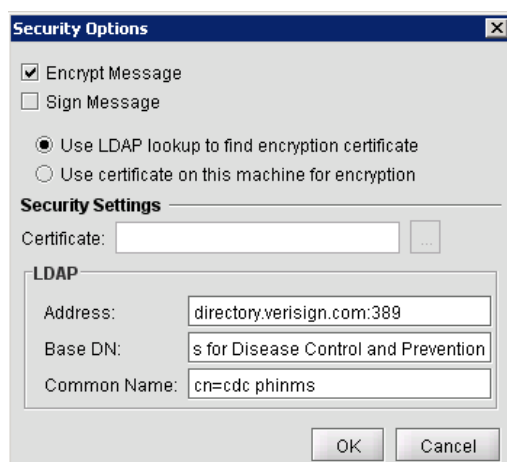


Figure 6.19. Security Options

Enter the following parameters:

- check Encrypt Message,
- select Use LDAP lookup to find encryption certificate,
- Address: directory.verisign.com:389,
- BaseDN: o=Centers for Disease Control and Prevention,
- Common Name: **cn=cdc phinms**,

Select OK,

Select Send displaying Figure 6.20, and

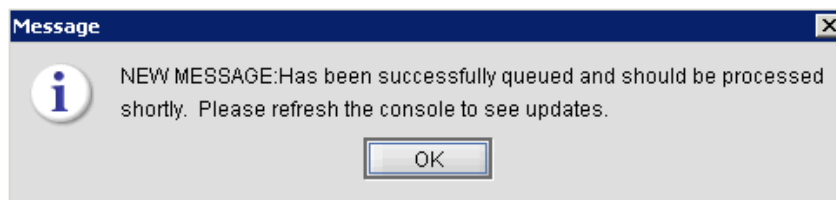


Figure 6.20. New Message Notification

Select OK.

6.7 Create Route Map

Messages sent using PHINMS need to address a specific recipient in the PHINMS 2.8.01 Console. Each Route is mapped to the recipient's attributes, such as the Uniform Resource Locator (URL), transport protocol, and authentication type. Obtain the partner's PartyID, the authentication type, and the security credentials.

Create a Route by completing the following steps:

1. Open the PHINMS 2.8.01 Console displaying Figure 6.21,

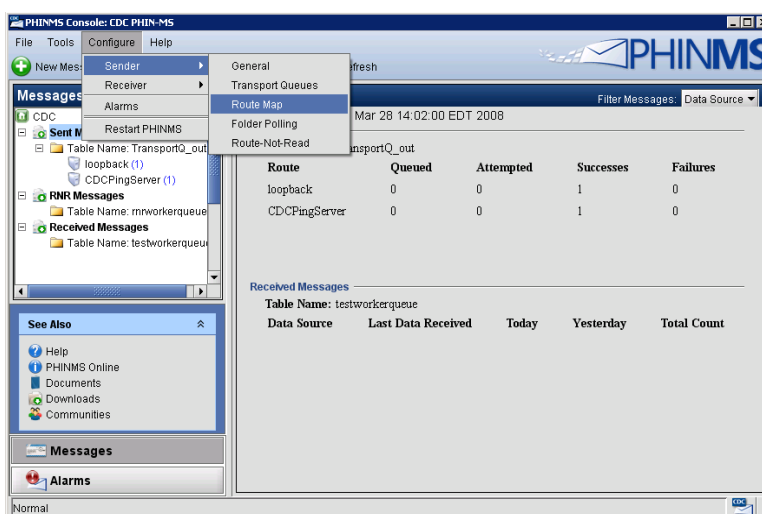


Figure 6.21. PHINMS 2.8.01 Console

2. Select Configure>Sender>Route Map displaying Figure 6.22,

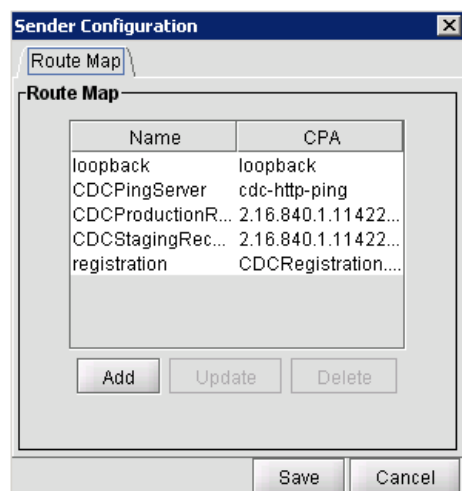
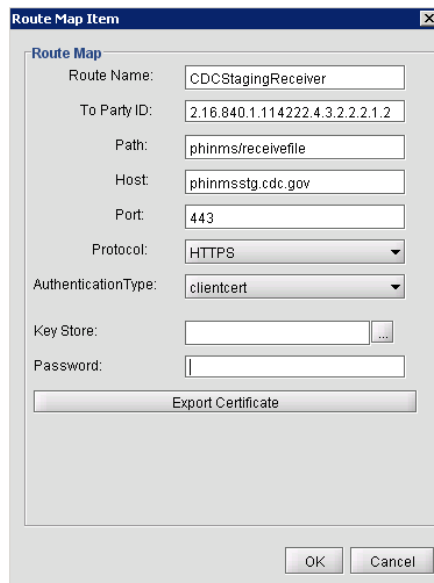


Figure 6.22. Route Map

3. Select Add displaying Figure 6.23,



The image shows a Windows-style dialog box titled "Route Map Item". It contains a "Route Map" section with the following fields: "Route Name" (text box with "CDCStagingReceiver"), "To Party ID" (text box with "2.16.840.1.114222.4.3.2.2.1.2"), "Path" (text box with "phinms/receivefile"), "Host" (text box with "phinmsstg.cdc.gov"), "Port" (text box with "443"), "Protocol" (dropdown menu with "HTTPS" selected), and "AuthenticationType" (dropdown menu with "clientcert" selected). Below these are "Key Store" (text box with a browse button "...") and "Password" (text box). At the bottom of the "Route Map" section is an "Export Certificate" button. At the bottom of the dialog box are "OK" and "Cancel" buttons.

Figure 6.23. Route Map Item

4. Enter the appropriate information in the following fields:

Enter Route Name,

Enter To Party ID,

Enter Path,

Enter Host,

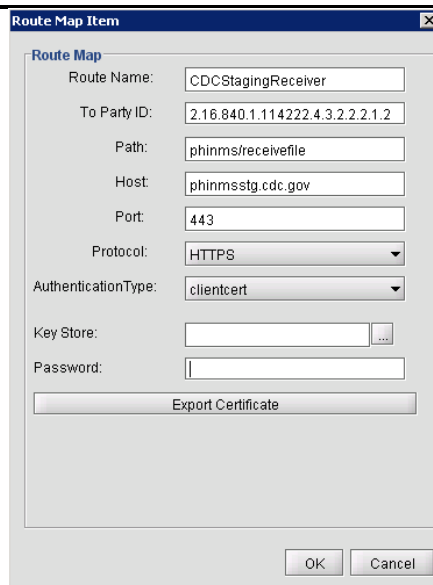
Enter Port,

Select Protocol,

Select Authentication Type, (for example, Client Cert)

6.8 Key Store Management Export certificate wizard

Note: “Export Certificate” is provide by keystore Management in efforts to provide a simpler way of exporting the .pfx or .cer files directly from the browser. Displaying figure 6.24,



Route Map Item

Route Map

Route Name: CDCStagingReceiver

To Party ID: 2.16.840.1.114222.4.3.2.2.1.2

Path: phinms/receivefile

Host: phinmsstg.cdc.gov

Port: 443

Protocol: HTTPS

AuthenticationType: clientcert

Key Store: []

Password: []

Export Certificate

OK Cancel

Figure 6.24. Route Map Item

5. Click “Export Certificate” displaying Figure 6.25,

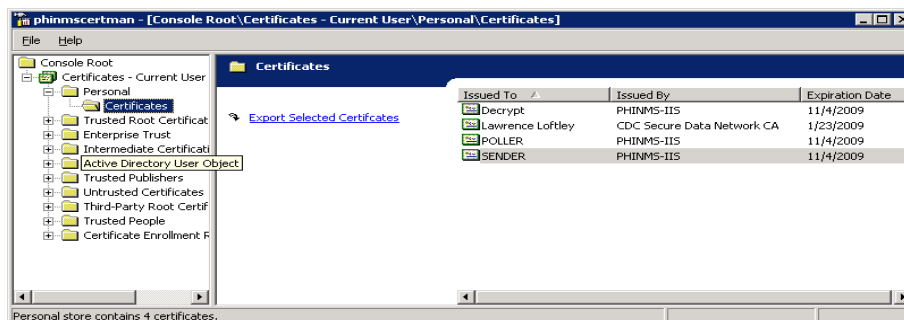


Figure 6.25. Windows MMC Certificates

6. Select a certificate form the list on the right and click “Export Selected Certificate”, displaying figure 6.26,



Figure 6.26. Certificate Export Wizard

7. Select Next displaying Figure 6.27,

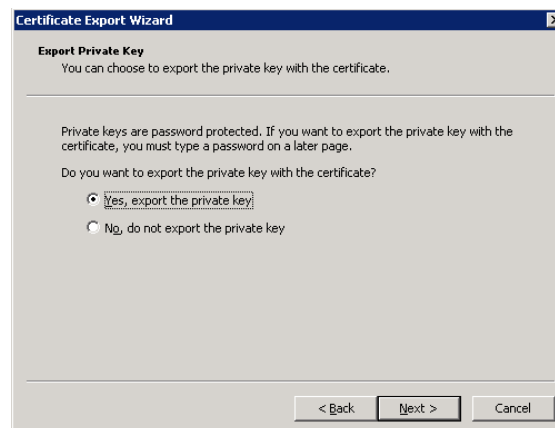


Figure 6.27. Export Private Key

7. Select Yes, export the private key,

8. Select Next displaying Figure 6.28,

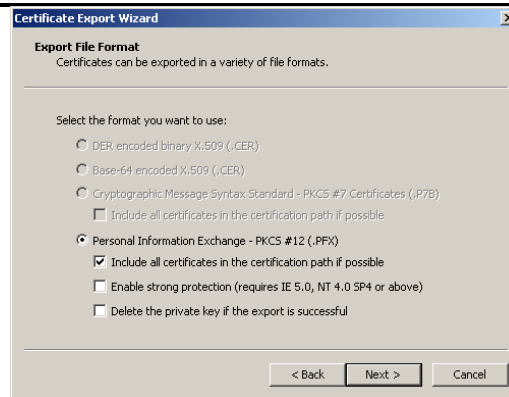


Figure 6.28. Export File Format

9. Select Personal information Exchange,
10. Check Include all certificates in the certification path if possible,
11. Uncheck Enable Strong Protection,
12. Uncheck Delete the private key if the export is successful,
13. Select Next displaying Figure 6.29,



Figure 6.29. Password

14. Enter and confirm the Password (SDN Challenge Phrase is recommended),
15. Select Next displaying Figure 6.30,



Figure 6.30. File to Export

16. Select Browse displaying Figure 6.31,

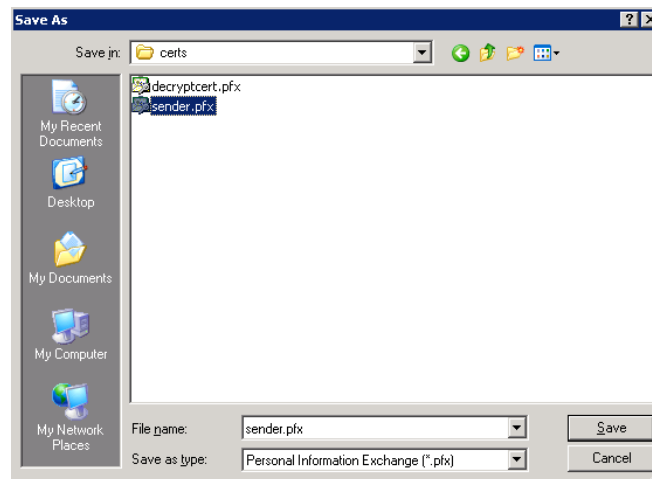


Figure 6.31. Save As

17. Navigate to C:\PHINMS install directory\ security\sender\name of the .pfx file,

18. Select Save displaying the File name on the File to Export screen,

19. Select Next,

20. Select Finish displaying Figure 6.32, and



Figure 6.32. Export was Successful

21. after inputting your .PFX and Password, displaying figure 6.33,

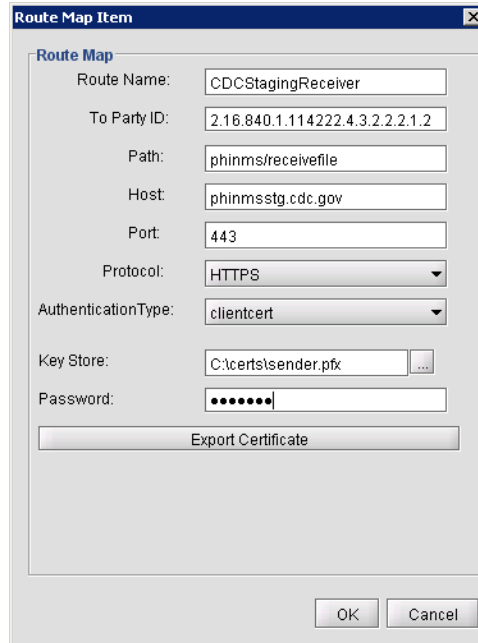


Figure 6.33. Route Map Item

Key Store Management Import certificate wizard

Perform the following steps to import a certificate:

Select elliptical to browse for your .pfx file displaying Figure 6.34,

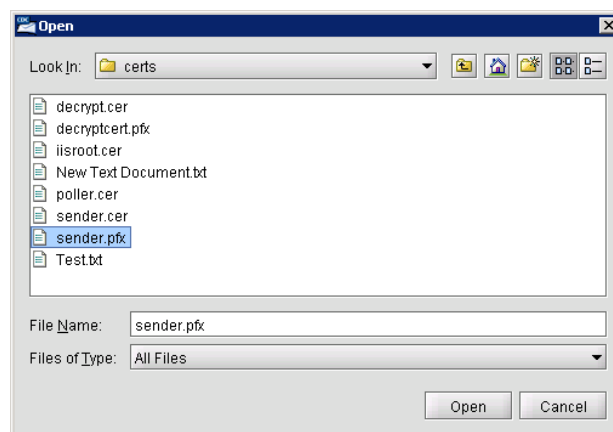
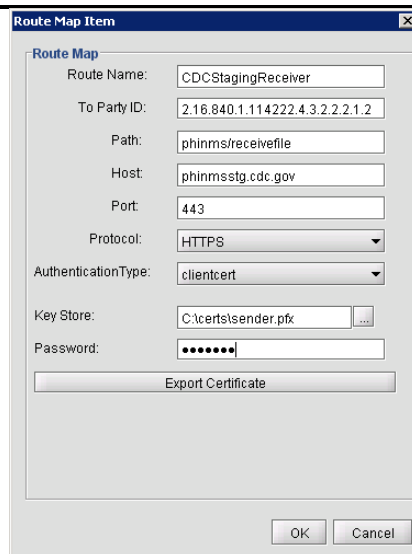


Figure 6.34. browse for .pfx file

Select OPEN, type password that was created for .pfx file, displaying figure 6.35,



Route Map Item

Route Map

Route Name: CDCStagingReceiver

To Party ID: 2.16.840.1.114222.4.3.2.2.2.1.2

Path: phinms/receivefile

Host: phinmsstg.cdc.gov

Port: 443

Protocol: HTTPS

AuthenticationType: clientcert

Key Store: C:\certs\sender.pfx

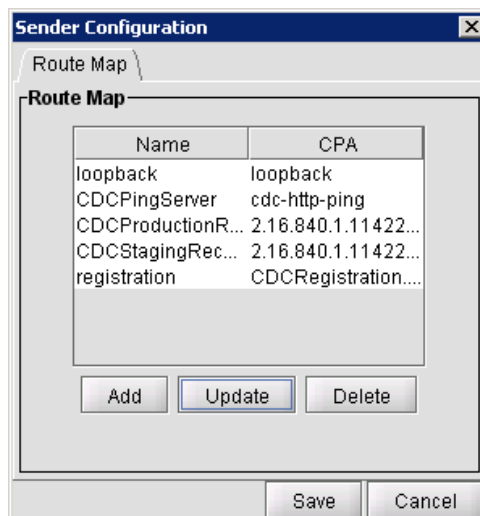
Password:

Export Certificate

OK Cancel

Figure 6.35. Route Map Item

Click OK, displaying figure 6.36,



Sender Configuration

Route Map

Route Map

Name	CPA
loopback	loopback
CDCPingServer	cdc-http-ping
CDCProductionR...	2.16.840.1.11422...
CDCStagingRec...	2.16.840.1.11422...
registration	CDCRegistration....

Add Update Delete

Save Cancel

Figure 6.36. Sender Configuration

Click Save, displaying figure 6.37,

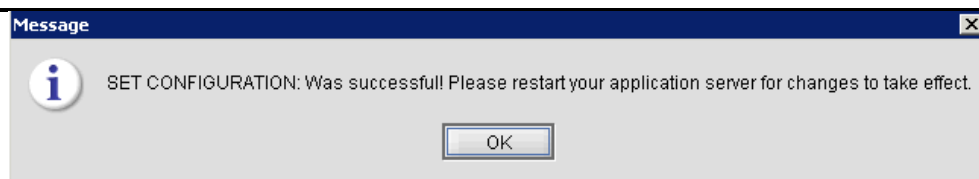


Figure 6.37. Set Configuration

Select OK, and

Restart PHINMS application from the console.

7.0 RECEIVER INFORMATION

7.1 Configure WorkerQ

The Worker Queue (WorkerQ) is the database table used for storing inbound messages. When configured from the Receiver configuration screen in the Console, it is used to drop incoming messages sent to the Receiver. The database configuration needs to be completed before creating WorkerQ table. The instructions to configure a database connection to the external database are in Section 5.0.

If configured from the Sender configuration screen in the Console, it is used to write the responses to polling requests (route-not-read configuration). More information on Sender configuration can be located in the PHINMS Technical Reference Guide.

Create an external database WorkerQ table by following steps below:

Open the PHINMS 2.8.01 Console displaying Figure 7.1,

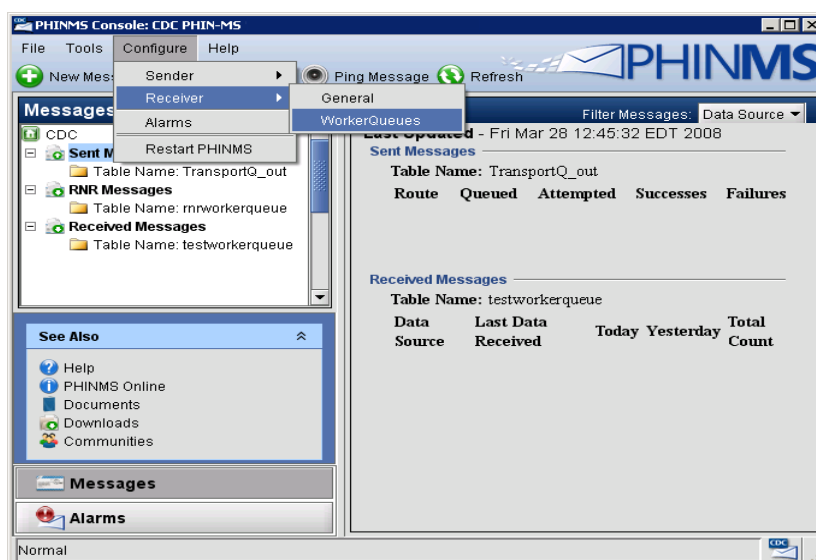


Figure 7.1. PHINMS 2.8.01 Console

Select Configure>Receiver>WorkerQueues displaying Figure 7.2,

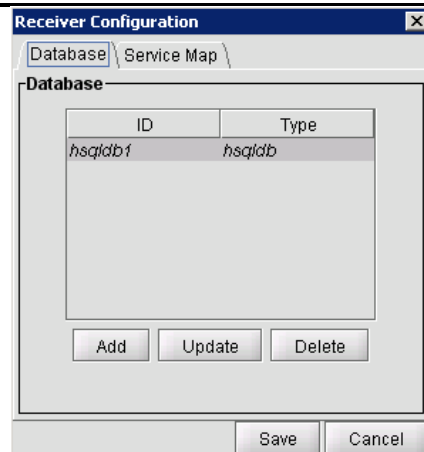
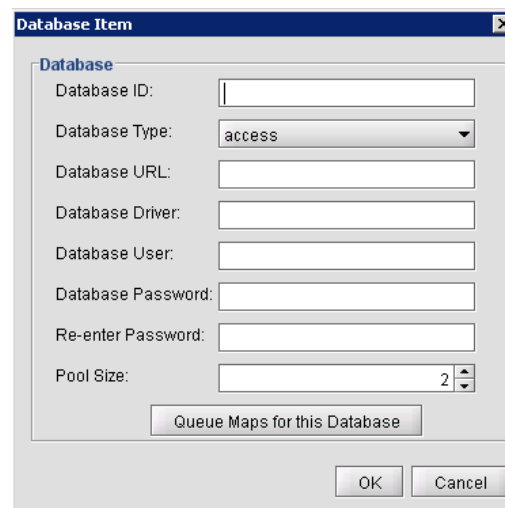


Figure 7.2. Receiver Configuration - Database

Select Add displaying Figure 7.3,



The 'Database Item' dialog box contains the following fields and controls:

- Database ID:** A text input field.
- Database Type:** A dropdown menu currently showing 'access'.
- Database URL:** A text input field.
- Database Driver:** A text input field.
- Database User:** A text input field.
- Database Password:** A text input field.
- Re-enter Password:** A text input field.
- Pool Size:** A spinner box currently set to '2'.
- Queue Maps for this Database:** A button.
- OK** and **Cancel** buttons at the bottom right.

Figure 7.3. Database Item

Enter the database items using Table 2 for an explanation of the values,

TAG VALUE	DESCRIPTION
Database ID	The unique name for the database connection pool, referenced in the queue map. The service map uses the databaseId to map the queue to a specific database. (The unique databaseId is determined by the user.)
Database Type	Designates the type of database.
Database URL	The URL to the database. The URL depends on the type of database and driver used such as jdbc:sqlserver://host:portnumber;DatabaseName=database for Microsoft SQL Server and jdbc:oracle://host:port:sid for Oracle.
Database Driver	The type of JDBC driver. The JDBC driver should be appropriate for the type of database such as com.microsoft.sqlserver.jdbc.SQLServerDriver for Microsoft

TAG VALUE	DESCRIPTION
	SQL Server and oracle.jdbc.OracleDriver for Oracle.
Database User	This user account is provided by the database administrator for login purposes which is used to automate the login process via PHINMS. A pointer to the database user entry in the Message Receiver's encrypted password store. The value is not the database user but the name of the tag within the password file. The value of the tag contains the actual database user name.
Database Password	This password is provided as part of the user account created by the database administrator for login purposes which is used to automate the login process via PHINMS. A pointer to the database password entry in the Message Receiver's encrypted password store. The value is not the database password but the tag within the password file. The value of the tag contains the actual database password.
Pool Size	The number of database connections to open. When setting the pool size ensure the system can handle the maximum client load while keeping enough memory available.

Table 2. WorkerQ Database Tag Values

Select Queue maps for this Database displaying Figure 7.4,

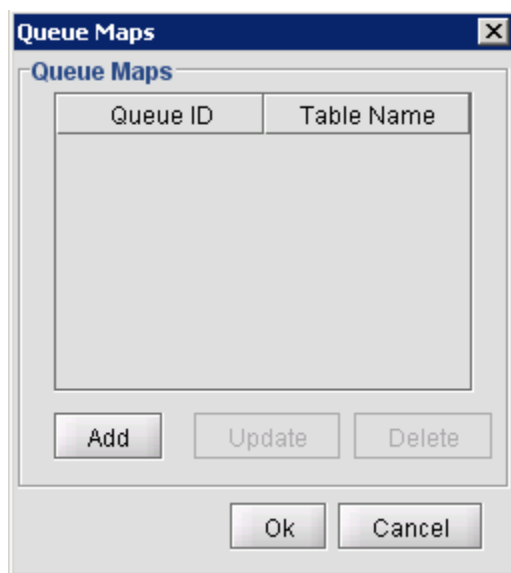


Figure 7.4. Queue Maps

Select Add displaying Figure 7.5,

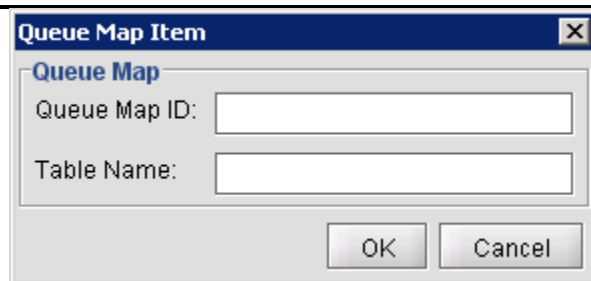


Figure 7.5. Queue Map Item

Enter Queue Map ID, (The Queue Map ID is determined by the user.)

Enter Table Name,

Click OK,

Click OK,

Click OK,

Click Save displaying Figure 7.6,

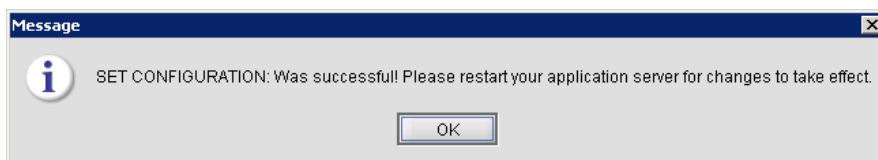


Figure 7.6. WorkerQ Database Configuration Successful

Select OK, and

Restart PHINMS.

7.2 Create Service and Action Pair

PHINMS 2.8.01 uses message envelopes for each sent message. The envelope has addressing information tags called Service and Action known as character strings. Character strings are logically mapped to an application queue on the receiving side. The Service and Action tags determine the message type.

Create a Service and Action pair by completing the following steps:

Open the PHINMS 2.8.01 Console displaying Figure 7.7,

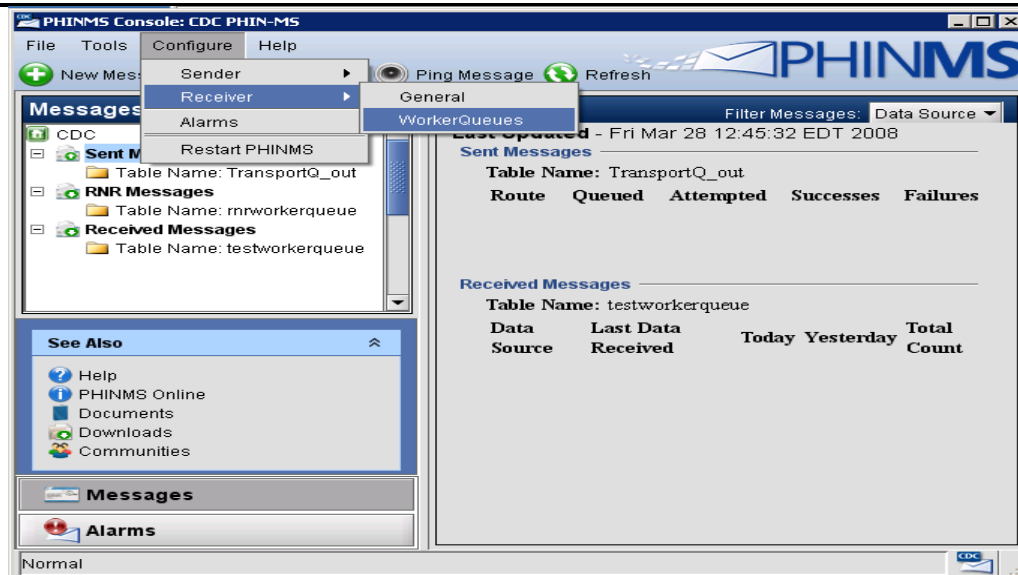


Figure 7.7. PHINMS 2.8.01 Console

Select Configure>Receiver>WorkerQueues displaying Figure 7.8,

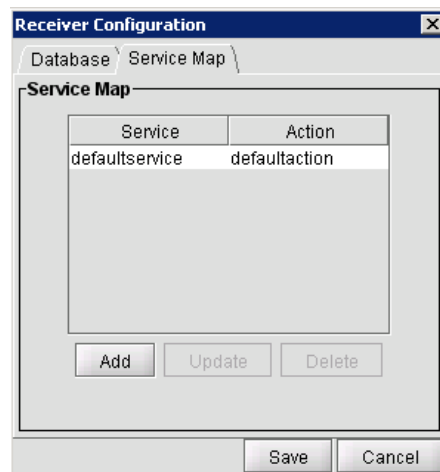


Figure 7.6. Service Map

Select Service Map,

Select Add displaying Figure 7.7,

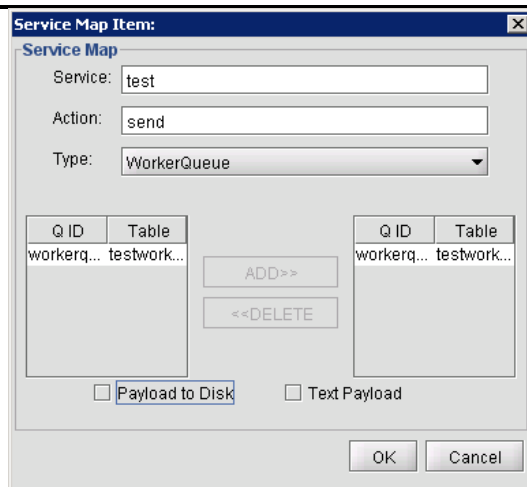


Figure 7.7. Service Map Item

Enter Service,

Enter Action,

Select WorkerQueue from the dropdown list,

Highlight workerqueue located under Q ID on the left-hand side,

Select Add,

Select OK displaying Figure 7.8,

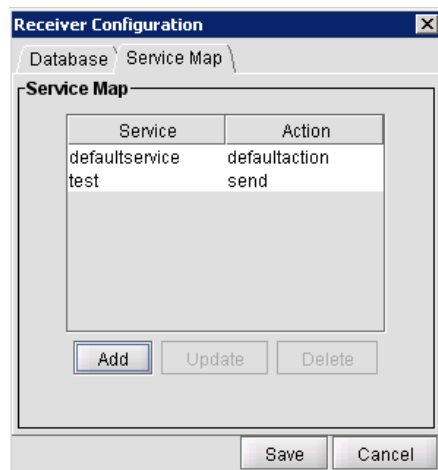


Figure 7.8. Service and Action Added

Select Save displaying Figure 7.9,

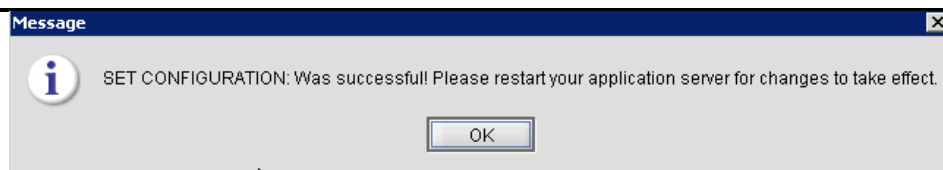


Figure 7.9. Service and Action Successful Configuration

Click OK, and

Restart PHINMS.

7.3 Configure Service Map

Open the PHINMS 2.8.01 Console displaying Figure 7.10,

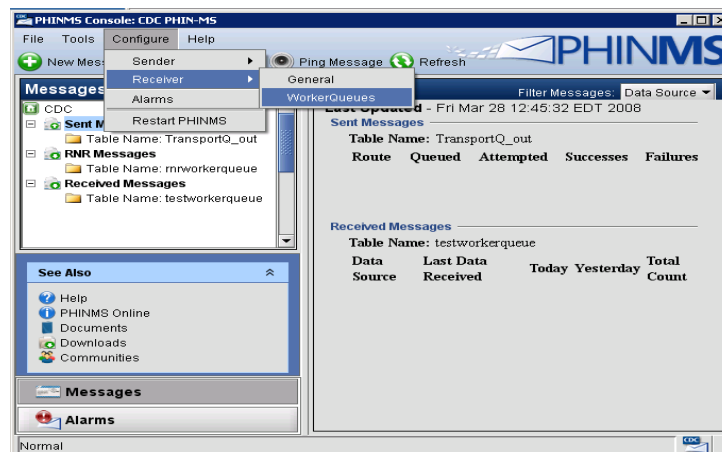


Figure 7.10. PHINMS 2.8.01 Console

Select Configure>Receiver>WorkerQueues displaying Figure 7.11,

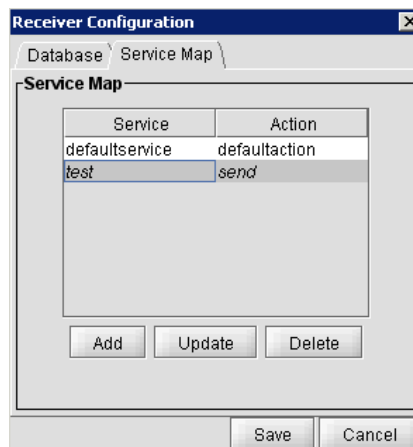
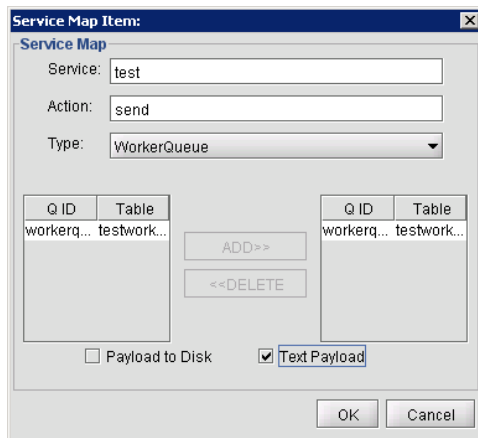


Figure 7.12. Service Map Receiver Configuration

Select Add, displaying Figure 7.13,



The dialog box is titled "Service Map Item:". It contains the following fields and controls:

- Service:** A text box containing the value "test".
- Action:** A text box containing the value "send".
- Type:** A dropdown menu currently showing "WorkerQueue".
- Tables:** Two tables are displayed side-by-side. Each table has two columns: "Q ID" and "Table". The left table contains one row with "workerq..." in the Q ID column and "testwork..." in the Table column. The right table also contains one row with "workerq..." in the Q ID column and "testwork..." in the Table column.
- Buttons:** Between the two tables are two buttons: "ADD>>" and "<<DELETE".
- Checkboxes:** At the bottom, there are two checkboxes: "Payload to Disk" (unchecked) and "Text Payload" (checked).
- OK/Cancel:** At the bottom right are "OK" and "Cancel" buttons.

Figure 7.13. Service Map Item

Enter the following parameters:

- Service: **test**,
- Action: **send**,
- Type: **WorkerQueue** opening the service map item,

Note: The Service and Type displayed in Figure 7.13 could use different terms depending on the program used.

Highlight testworkerqueue QID,

Select Add moving the Q ID to the right,

Check Text Payload,

Note: When Payload to Disk is checked the incoming payload is written to disk instead of to the database field. In this case the name of the local file on disk is stored in the WorkerQ table. When Text Payload is checked, the payload is written to the **payloadTextContent** field. When Text Payload is not checked, the payload is written to the **payloadBinaryContent** field in the WorkerQ.

Select OK, and

Select Save returning to the PHINMS 2.8.01 Console.

Send a dummy message to test the setup. Verify the TransportQ and WorkerQ data fields are correct.

8.0 UNINSTALL PHINMS 2.8.01

Complete the following steps to uninstall PHINMS 2.8.01:

1. Select Start>Programs>PHINMS>Uninstall PHINMS displaying Figure 8.1,

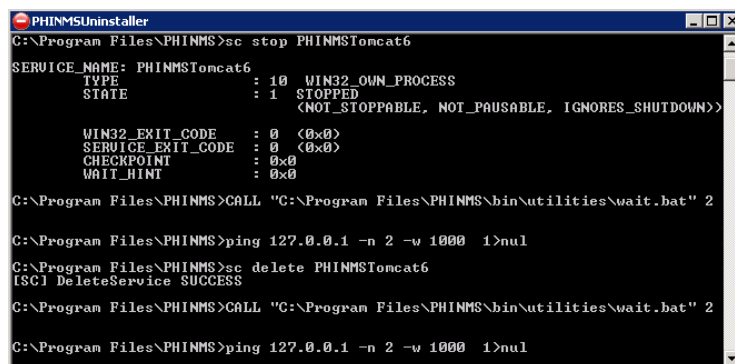


Figure 8.1. PHINMS Uninstaller screen

2. The DOS window displays the services are stopped and deleted at which time the application uninstaller screen is initiated displaying Figure 8.2,

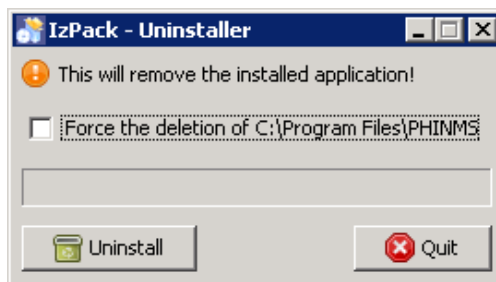


Figure 8.2. Application Uninstaller

3. Select “Force the deletion of the PHINMS install directory folder structure” then click Uninstall displaying Figure 8.3, and

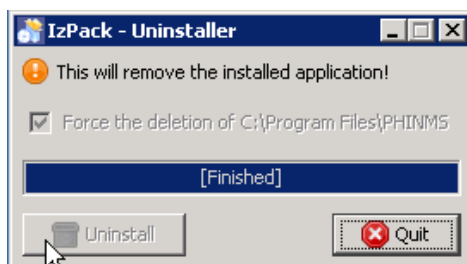


Figure 8.3. Successful Uninstall

4. Click Quit.

5. Navigate to the PHINMS install directory displaying Figure 8.4,

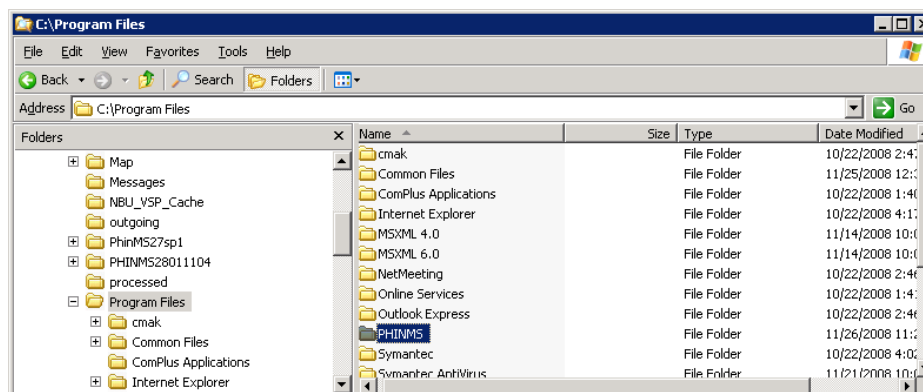


Figure 8.4. PHINMS install directory

6. Delete the PHINMS install directory. You have successfully uninstalled PHINMS 2.8.01.

9.0 ADDITIONAL FEATURES

9.1 Export CPA

PHINMS 2.8.01 allows the user to export the Collaboration Protocol Agreement (CPA) directly from the PHINMS 2.8.01 Console. Complete the following steps to export the CPA:

- Open the PHINMS 2.8.01 Console,
- Select Tools,
- Select Export CPA Files,
- Select the Route(s) to export,
- Select Export Selected Routes,
- Select a folder to store the exported CPA,
- Select Open, and
- Select OK.

9.2 Import CPA

PHINMS 2.8.01 allows the user to import the CPA directly from the PHINMS 2.8.01 Console. Complete the following steps to import the CPA:

- Open the PHINMS 2.8.01 Console,
- Select Tools,
- Select Import CPA,
- Select the CPA to import,
- Select Open, and
- Select OK.

9.3 View Receiver Logs

The Receiver Logs stores information on the status of received messages and can be viewed directly from the PHINMS 2.8.01 Console. Viewing the logs allows users to check the status of received messages. Complete the following steps to view the Receiver Logs:

- Open the PHINMS 2.8.01 Console,
- Select Tools,
- Select Receiver Logs,
- Select the Route from the drop-down list,
- Select Date, and
- Select View displaying the text.

9.4 View Sender Logs

The Sender Logs stores information on the status of send messages and can be viewed directly from the PHINMS 2.8.01 Console. Viewing the logs allows users to check the status of sent messages. Complete the following steps to view the Sender Logs:

- Open the PHINMS 2.8.01 Console,
- Select Tools,
- Select View Sender Logs,
- Select Route from the drop-down list,
- Select Date, and
- Select View displaying the text.

9.5 Import Trusted Certificate

A Trusted Certificate consists of a root and intermediate CA certificate. When the browser is trying to make an SSL connection, it needs to validate the Certificate Chain of the SSL certificate installed on the proxy server on the Receiver's end. PHINMS Sender verifies the Chain using CACERTS Key Store file. If the Chain does not match, the Sender has to import the Trusted Certificate into the CACERTS Key Store file by using an import option

The user can now import the Trusted Certificate directly from the PHINMS 2.8.01 Console. Complete the following steps to import the Trusted Certificate:

- Open the PHINMS 2.8.01 Console,
- Select Tools,
- Select Import Trusted Cert,
- Navigate to the location the Trusted Certificate is stored,
- Select the Trusted Certificate (.cer or .pem file) to import, and
- Select Open, successfully importing the Trusted Certificate into the Sender's trusted CA certificate store.

9.6 Import JDBC JAR Files

JDBC Jar Files are able to be imported directly from the PHINMS 2.8.01 Console. Complete the following steps to import the three (3) JDBC Jar Files:

- Open the PHINMS 2.8.01 Console,
- Select Tools,
- Select Import JDBC Jar Files,
- Locate and select the jdbc driver for your database (see Table 1. JDBC Drivers, section 2.1, page 11 for recommended jdbc drivers)

Select Open,

A message will indicate a successful import, select OK, and

Restart PHINMS Tomcat Instance located in the Windows services console.

9.7 Change Login Password

PHINMS 2.8.01 allows the user to change the Console login password. Complete the following steps to successfully change the login password:

Open the PHINMS 2.8.01 Console,

Select File,

Select Change Login Password,

Enter the Old Console Password,

Enter the New Console Password and Re-Enter New Console Password,

Select Change Password,

Click OK, and

Restart PHINMS 2.8 Apache Tomcat service.

9.8 Sender and Receiver Alarms

PHINMS 2.8.01 contains system alarms for the Sender and Receiver. This feature allows the user to acknowledge and enter a resolution for each alarm. Configure the alarm features by completing the following steps:

Open the PHINMS 2.8.01 Console,

Select Configure, Alarms,

Check Report Alarms

Note: When the Report Alarms is selected, the alarms can be viewed in the Console and enabling the configuration of the Email Alarms feature.

Complete the following fields:

- **SMTP Server** - required,
- User Name,
- User Password,
- Re Enter User Password,
- **From Address** - required,

Select OK.

9.9 Alarm Resolution

The Alarm Resolution feature allows the user to view error and help messages. It also allows the user to store the resolution information. Take advantage of the Alarm Resolution feature by completing the following steps:

Open the PHINMS 2.8.01 Console, Select Alarms located at the lower left-hand side of the console displaying Figure 9.1,

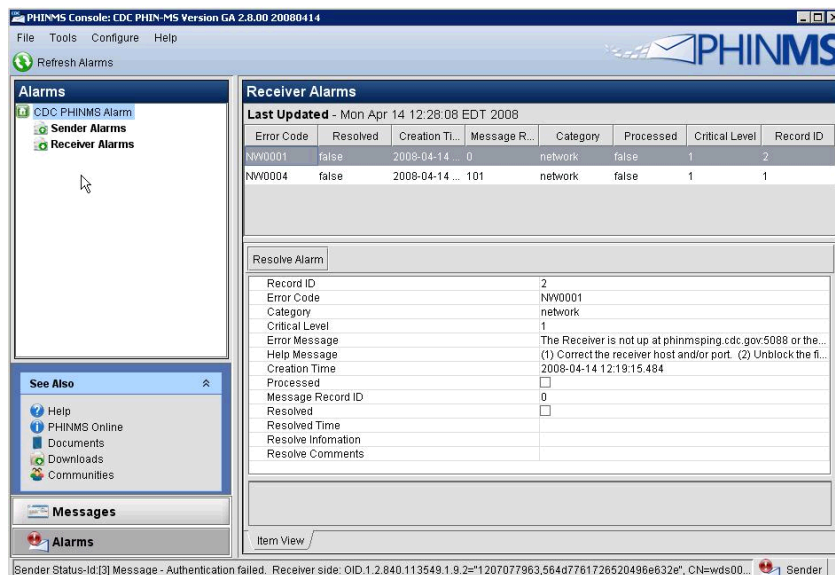


Figure 9.1. Alarms

Select the Message to review,

Select Resolve Alarms displaying Figure 9.2,

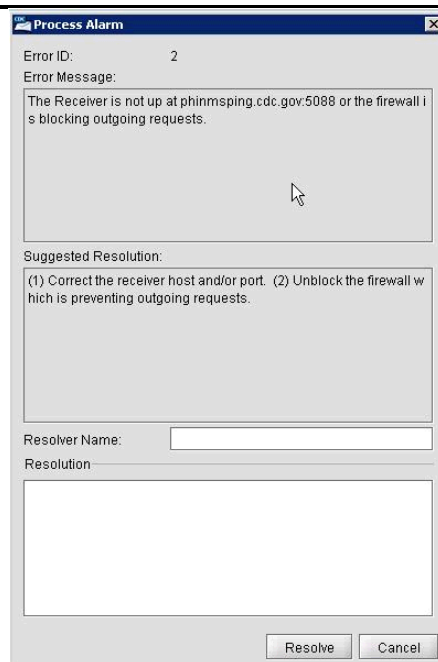


Figure 9.2. Alarm Resolution

Review the Error Message and the Suggested Resolution,
 Enter the Resolver Name,
 Enter the Resolution,
 Select Resolve displaying Figure 9.3, and



Figure 9.3. Alarm Successfully Processed

Select OK.

9.10 Folder-Based Polling

This feature makes it much easier for applications to interface with PHINMS 2.8.01. Senders can now configure the Console for Folder-Based Polling. Folder Based Polling allows the Sender to store the messages in a folder and the system will send the messages from the folder instead of a database. The associated route is defined in the Console and does not need file descriptors. Configure the Folder Based Polling feature by completing the following steps:

open the PHINMS 2.8.01 Configure,

select Configure>Sender>Folder Polling,
check Folder Based Polling,
select Add,
populate the Folder Properties,
select Security Options,
select OK,
select Save,
select OK,
select the PHINMS 2.8.01 Console Restart button,
create the following three (3) folders in any directory:

- **Outgoing** - used to store messages to be sent,
- **Processed** - regional file which messages have been processed, and
- **Acknowledgement** - stores the message receipt from the Receiver.

9.11 Transport Queue Auto Delete

open the PHINMS 2.8.01 Configure,
select Configure>Sender>TransportQueues
Select the Transport Queue to be modified
Click update
Click Queues for this database
Select the table to be modified
Click update
Locate the auto delete section
Enable Auto delete
Modify Frequency to your desired setting
Configure a start date and time
Modify Retention Period to your desired setting
Click ok, click ok, click ok, click save
Click ok on the acknowledgement
Click configure
Click Restart PHINMS

9.12 Worker Queue Auto Delete

open the PHINMS 2.8.01 Configure,
select Configure>Receiver>WorkerQueues
Select the WorkerQueues to be modified
Click update
Click Queues for this database
Select the table to be modified
Click update
Locate the auto delete section
Enable Auto delete
Modify Frequency to your desired setting
Configure a start date and time
Modify Retention Period to your desired setting
Click ok, click ok, click ok, click save
Click ok on the acknowledgement
Click configure
Click Restart PHINMS

■